Innominate mGuard

Benutzerhandbuch

Software-Release 6.1.0

Innominate Security Technologies AG
Albert-Einstein-Str. 14
D-12489 Berlin
Tel.: +49 (0)30 6392 3300
contact@innominate.de
www.innominate.de

Copyright © 2008 Innominate Security Technologies AG

September 2008
„Innominate“ und „mGuard“ sind registrierte Handelsnamen der Innominate Security Technologies AG. Die mGuard Technologie ist durch die Patente 10138865 und 10305413, erteilt durch „Deutsches Patent- und Markenamt“, geschützt. Weitere Patente sind angemeldet.
Weder das Gesamtdokument noch Teile davon dürfen ohne schriftliche Genehmigung übertragen oder kopiert werden.
Die Innominate Security Technologies AG behält sich das Recht vor, jederzeit und ohne Benachrichtigung dieses Dokument zu verändern.
Die Innominate Security Technologies AG übernimmt ferner keine Haftung für Fehler im vorliegenden Dokument sowie für zufällige oder Folgeschäden im Zusammenhang mit der Lieferung, Leistung oder Verwendung dieser Unterlagen.
Ohne die vorherige schriftliche Zustimmung der Innominate Security Technologies AG darf dieses Handbuch weder teilweise noch vollständig fotokopiert, vervielfältigt oder in eine andere Sprache übersetzt werden.

Innominate Dokumentennummer: UG206001108-014

Inhalt

1 Einleitung 9
Netzwerk-Features 9
Firewall-Features 9
Anti-Virus-Features 9
VPN-Features 10
Weitere Features 10
Support 10
1.1 Geräteversionen 11
mGuard industrial RS 11
mGuard smart 11
mGuard PCI 11
mGuard blade 11
EAGLE mGuard 12
mGuard delta 12
2 Typische Anwendungsszenarien 13
Stealth-Modus 13
Netzwerkrouter 13
DMZ 13
VPN Gateway 14
WLAN über VPN 14
Auflösen von Netzwerkkonflikten 15
3 Bedienelemente und Anzeigen 16
3.1 mGuard industrial RS 16
3.2 mGuard smart 17
3.3 mGuard PCI 18
3.4 mGuard blade 19
3.5 EAGLE mGuard 20
3.6 mGuard delta 21
4 Inbetriebnahme 22
Sicherheits-
hinweise 22
Allgemeine Hinweise zur Benutzung 22
Schritte zur Inbetriebnahme 22
Zum Lieferumfang gehören 23
4.1 mGuard industrial RS installieren 24
Montage 24
Demontage 24
Anschlüsse 25
4.2 mGuard smart anschließen 30
4.3 mGuard blade installieren 31
mGuard bladeBase installieren 31
mGuard blade installieren 31
Kontrolleinheit (CTRL Slot) 31
Anschluss mGuard blade 32
4.4 EAGLE mGuard installieren 33
Klemmblock 33
Montage 34
Inbetriebnahme 35
Netzwerkverbindung 35
Demontage 35
4.5 mGuard delta anschließen 36
4.6 mGuard PCI installieren 37

4.6.1 Auswahl Treibermodus oder Power-over-PCI Modus ... 37
Treibermodus ... 37
Power-over-PCI Modus ... 39
4.6.2 Einbau der Hardware ... 40
4.6.3 Treiberinstallation ... 41
Voraussetzungen ... 41
Unter Windows XP ... 41
Unter Windows 2000 ... 42
Unter Linux ... 45

5 Konfiguration vorbereiten ... 46
5.1 Anschlussvoraussetzungen ... 46
mGuard industrial RS ... 46
mGuard smart ... 46
mGuard PCI ... 46
mGuard blade ... 46
EAGLE mGuard ... 46
mGuard delta ... 47
5.2 Lokale Konfiguration: Bei Inbetriebnahme ... 48
5.2.1 mGuard industrial RS, mGuard smart, mGuard blade und EAGLE mGuard ... 48
Bei konfigurierter Netzwerkschnittstelle ... 48
Bei nicht konfigurierter Netzwerkschnittstelle ... 48
5.2.2 mGuard delta ... 50
5.2.3 mGuard PCI ... 51
Installieren der PCI Karte ... 51
Installieren der Treiber ... 51
Konfiguration der Netzwerkschnittstelle ... 51
Standardgateway ... 51
5.3 Lokale Konfigurationsverbindung herstellen ... 53
Web-basierte Administratoroberfläche ... 53
Bei erfolgreichem Verbindungsaufbau ... 54
5.4 Fernkonfiguration ... 56
Voraussetzung ... 56
Fernkonfiguration ... 56

6 Konfiguration ... 57
6.1 Bedienung ... 57
6.2 Menü Verwaltung ... 60
6.2.1 Verwaltung » Systemeinstellungen ... 60
Host ... 60
Meldekontakt (nur mGuard industrial RS, EAGLE mGuard) ... 62
Zeit und Datum ... 63
Shell-Zugang ... 67
6.2.2 Verwaltung » Web Einstellungen ... 74
Grundeinstellungen ... 74
Zugriff ... 75
6.2.3 Verwaltung » Lizenzierung ... 82
Übersicht ... 82
Installieren ... 83
Lizenzbedingungen ... 84
6.2.4 Verwaltung » Update ... 85
Übersicht ... 85
Update ... 86
Anti-Virus Muster ... 88
6.2.5 Verwaltung » Konfigurationsprofile ... 89
Konfigurationsprofile ... 89

Profile auf dem ACA
(nur EAGLE mGuard) ... 90
6.2.6 Verwaltung » SNMP ... 92
Abfrage ... 92
Trap ... 95
LLDP ... 101
6.2.7 Verwaltung » Zentrale Verwaltung ... 102
Konfiguration holen ... 102
6.2.8 Verwaltung » Neustart ... 105
Restart ... 105
6.3 Menü Bladekontrolle (nur blade Kontroller) ... 106
6.3.1 Bladekontrolle » Übersicht ... 106
6.3.2 Bladekontrolle » Blade 01 bis 12 ... 107
Blade in slot # ... 107
Konfiguration ... 108
6.4 Menü Netzwerk ... 109
6.4.1 Netzwerk » Interfaces ... 109
Allgemein ... 110
» Netzwerk-Modus: Stealth ... 120
» Netzwerk-Modus: Router ... 123
» Netzwerk-Modus: PPPoE ... 125
» Netzwerk-Modus: PPTP ... 126
» Netzwerk-Modus: Modem / Eingebautes Modem ... 127
Netzwerk Modus » Router, PPPoE, PPTP oder Modem / Eingebautes Modem ... 128
Ethernet ... 129
Ausgehender Ruf ... 131
Eingehender Ruf ... 136
Modem / Konsole ... 139
6.4.2 Netzwerk » NAT ... 145
Masquerading ... 145
Portweiterleitung ... 147
6.4.3 Netzwerk » DNS ... 149
DNS Server ... 149
DynDNS ... 152
6.4.4 Netzwerk » DHCP ... 153
Internes / Externes DHCP ... 153
6.4.5 Netzwerk » Proxy-Einstellungen ... 157
HTTP(S) Proxy- Einstellungen ... 157
6.5 Menü Authentifizierung ... 158
6.5.1 Authentifizierung » Lokale Benutzer ... 158
Passworte ... 158
6.5.2 Authentifizierung » Firewall-Benutzer ... 160
Firewall-Benutzer ... 160
RADIUS-Server ... 161
Zugriff ... 161
Status ... 162
6.5.3 Authentifizierung » Zertifikate ... 163
Erstellung von Zertifikaten ... 165
Authentifizierungsverfahren ... 165
Zertifikatseinstellungen ... 167
Maschinenzertifikate ... 169
CA-Zertifikate ... 171
Gegenstellenzertifikate ... 172
CRL ... 175

6.6 Menü Netzwerksicherheit (nicht blade Kontroller) ... 177
6.6.1 Netzwerksicherheit » Paketfilter ... 177
Eingangsregeln ... 177
Ausgangsregeln ... 179
Regelsätze ... 180
Regelsatz ... 181
MAC Filter ... 183
Erweiterte Einstellungen ... 184
6.6.2 Netzwerksicherheit » DoS-Schutz ... 188
Flood Protection ... 188
6.6.3 Netzwerksicherheit » Benutzerfirewall ... 190
Benutzerfirewall-Templates ... 190
Benutzerfirewall » Template editieren ... 190
Allgemein ... 191
Template Benutzer ... 192
Firewall Regeln ... 193
6.7 Menü Web-Sicherheit (nicht blade Kontroller) ... 194
6.7.1 Web-Sicherheit » HTTP ... 194
Virenschutz ... 194
6.7.2 Web-Sicherheit » FTP ... 197
Virenschutz ... 197
6.8 Menü E-Mail-Sicherheit (nicht blade Kontroller) ... 200
6.8.1 E-Mail-Sicherheit » POP3 ... 200
Virenschutz ... 200
6.8.2 E-Mail-Sicherheit » SMTP ... 203
Virenschutz ... 203
6.9 Menü IPsec VPN (nicht blade Kontroller) ... 206
6.9.1 IPsec VPN » Global ... 206
Optionen ... 206
DynDNS-Überwachung ... 211
6.9.2 IPsec VPN » Verbindungen ... 212
Verbindungen ... 212
6.9.3 VPN-Verbindung / VPN-Verbindungskanäle definieren ... 214
Allgemein ... 214
Allgemein ... 219
Authentifizierung ... 222
Firewall ... 227
IKE-Optionen ... 229
6.9.4 IPsec VPN » L2TP über IPsec ... 232
L2TP Server ... 232
6.9.5 IPsec VPN » IPsec Status ... 233
6.10 Menü SEC-Stick ... 235
6.10.1 Global ... 235
Zugriff ... 235
6.10.2 Verbindungen ... 238
SEC-Stick Verbindungen ... 238
6.11 Menü QoS ... 240
6.11.1 Ingress Filter ... 240
Intern / Extern ... 240
6.11.2 Egress Queues ... 243
Intern / Extern / Extern 2 / Einwahl ... 243
6.11.3 Egress Queues (VPN) ... 244
VPN via Intern / VPN via Extern / VPN via Extern 2 / VPN via Einwahl ... 244
6.11.4 Egress Zuordnungen ... 246

Intern / Extern / Extern2 / Einwahl ... 246
6.11.5 Egress Zuordnungen VPN ... 247
VPN via Intern / VPN via Extern / VPN via Extern2 / VPN via Einwahl ... 247
6.12 Menü Redundanz ... 250
6.12.1 Firewall-Redundanz ... 250
Redundanz ... 251
ICMP Checks ... 252
6.12.2 Ring-/Netzkopplung ... 253
Ring-/Netzkopplung ... 253
6.13 Menü Logging ... 254
6.13.1 Logging » Einstellungen ... 254
Remote Logging ... 254
6.13.2 Logging » Logs ansehen ... 256
Kategorien der Log-Einträge ... 256
6.14 Menü Support ... 260
6.14.1 Support » Werkzeuge ... 260
Ping Check ... 260
Traceroute ... 260
DNS Lookup ... 260
IKE Ping ... 261
6.14.2 Support » Erweitert ... 262
Hardware ... 262
Snapshot ... 262
6.15 CIDR (Classless Inter-Domain Routing) ... 263
6.16 Netzwerk-Beispielskizze ... 264
7 Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware ... 265
7.1 Neustart durchführen ... 265
7.2 Recovery-Prozedur ausführen ... 265
7.3 Flashen der Firmware ... 266
Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server ... 268
7.3.1 DHCP- und TFTP-Server unter Windows oder Linux installieren ... 269
Unter Windows ... 269
Unter Linux ... 270
8 Glossar ... 271
Asymmetrische Verschlüsselung ... 271
DES / 3DES ... 271
AES ... 271
CA-Zertifikat ... 271
Client / Server ... 272
Datagramm ... 272
Default Route ... 272
DynDNS-Anbieter ... 273
IP-Adresse ... 273
IPsec ... 274
Subject, Zertifikat ... 275
NAT (Network Address Translation) ... 276
Port-Nummer ... 276
Proxy ... 277
PPPoE ... 277
PPTP ... 277
Router ... 277
Trap ... 277
X.509 Zertifikat ... 277
Protokoll, Übertragungsprotokoll ... 278

Service Provider 278
Spoofing, Antispoofing 278
Symmetrische Verschlüsselung 278
TCP/IP (Transmission Control Protocol/Internet Protocol) 278
VLAN 279
VPN (Virtuelles Privates Netzwerk) 279

9 Technische Daten 280
Allgemein 280
mGuard industrial RS 280
EAGLE mGuard 281

1 Einleitung

Der mGuard sichert IP-Datenverbindungen. Dazu vereinigt das Gerät folgende Funktionen:

- Netzwerkkarte (mGuard PCI), Switch (mGuard delta)
- VPN-Router (VPN - Virtuelles Privates Netzwerk) für sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES, 3DES und AES Verschlüsselung, IPsec Protokoll)
- Konfigurierbare Firewall für den Schutz vor unberechtigtem Zugriff. Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr.
- Virenschutz mit Unterstützung für die Protokolle HTTP, FTP, SMTP und POP3

Die Konfiguration des Gerätes erfolgt einfach mit einem Web-Browser.

Für weiterführende Informationen:
– Siehe Webseite von Innominate: www.innominate.de (zusammen mit weiteren Dokumenten)

Netzwerk-Features

- Stealth (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (für DSL), PPTP (für DSL) und Modem
- VLAN
- DHCP Server/Relay auf den internen und externen Netzwerkschnittstellen
- DNS Cache auf der internen Netzwerkschnittstelle
- Administration über HTTPS und SSH
- Optionales Umschreiben von DSCP/TOS-Werten (Quality of Service)
- Quality of Service (QoS)
- LLDP
- MAU Management

Firewall-Features

- Stateful Packet Inspection
- Anti-Spoofing
- IP Filter
- L2 Filter (nur im Stealth Mode)
- NAT mit FTP, IRC und PPTP Unterstützung (nur in den Router-Modi)
- 1:1 NAT (nur im Netzwerkmodus *Router*)
- Port Forwarding (nicht im Netzwerkmodus *Stealth*)
- Individuelle Firewallregeln für verschiedene Nutzer (Benutzerfirewall)
- Individuelle Regelsätze als Aktion (Ziel) von Firewallregeln (ausgenommen Benutzerfirewall oder VPN Firewall)
- Firewalldurchsatz maximal 99MBit/s

Anti-Virus-Features

- ClamAV-Virenschutz
- Unterstützte Protokolle: HTTP, FTP, POP3 und SMTP (senden)
- Der Virenfilter kann die folgenden Formate dekomprimieren:
    - ZIP
    - RAR
    - GZIP
    - BZIP2
    - TAR
    - MS OLE2
    - MS CHM (Komprimiertes HTML)
    - MS SZDD

- UPX
- FSG
- Petite

VPN-Features

- Protokoll: IPsec (Tunnel und Transport Mode)
- IPsec Verschlüsselung in Hardware mit DES (56 Bit), 3DES (168 Bit), AES (128, 192, 256 Bit)
- Paket-Authentifizierung: MD5, SHA-1
- Internet Key Exchange (IKE) mit Main und Quick Mode
- Authentisierung über
  - Pre-Shared Key (PSK)
  - X.509v3 Zertifikate mit
    - Public Key Infrastruktur (PKI) mit Certification Authority (CA), optionaler Certificate Revocation List (CRL) und Filtermöglichkeit nach Subjects

    oder
    - Zertifikat der Gegenstelle, z. B. selbstunterschriebene Zertifikate
- Erkennen wechselnder IP Adressen von Gegenstellen über DynDNS
- NAT-Traversal (NAT-T)
- Dead Peer Detection (DPD): Erkennung von IPsec Verbindungsabbrüchen
- IPsec/L2TP Server: Anbindung von IPsec/L2TP Clients
- IPsec Firewall und 1:1 NAT
- Defaultroute über VPN
- Weiterleiten von Daten zwischen VPNs (Hub and Spoke)
- Bis zu 250 VPN Tunnel
- VPN Durchsatz max. 35MBit/s bei 266MHz und 70MBit/s bei 533MHz mGuard

Weitere Features

- Remote Logging
- Router/Firewall Redundanz
- Administration unter Benutzung von SNMP v1-v3 und Innominate Device Manager (IDM)
- PKI-Unterstützung für HTTPS/SSH Remote Access
- Kann über die LAN-Schnittstelle als NTP- und DNS-Server agieren

Support

Bei Problemen mit Ihrem mGuard wenden Sie sich bitte an Ihren Händler. Zusätzliche Informationen zum Gerät, sowie Release Notes und Software-Updates finden Sie unter folgender Internet-Adresse: http://www.innominate.de/

1.1 Geräteversionen

Den mGuard gibt es in folgenden Geräteausführungen, deren Funktionen weitgehend identisch sind. Alle Geräte sind einsetzbar unabhängig davon, welche Prozessor-Technologie und welches Betriebssystem die angeschlossenen Rechner benutzen.

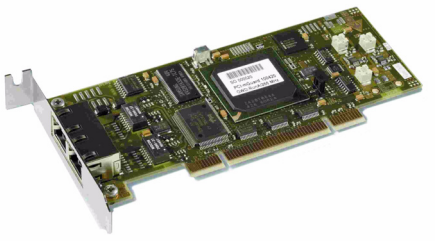
mGuard industrial RS

Der mGuard industrial RS ist in drei Geräteversionen lieferbar: mit integriertem Modem, mit integriertem ISDN-Terminaladapter oder ohne diese Geräte. Er ist dadurch hybrid nutzbar als Firewall/VPN Router sowohl über Ethernet als auch für serielle Wählverbindungen. Der Namenszusatz „RS“ besagt, dass dieses Gerät in besonderer Weise für gesicherte Remote Services (Ferndiagnose, Fernkonfiguration, Teleservice) geeignet ist. Das Gerät ist konzipiert für die Montage auf Hutschienen (gemäß DIN EN 50 022) und ist damit vor allem für den Einsatz im industriellem Umfeld geeignet.
VPN-Tunnel können per Software- oder Hardware-Schalter initiiert werden. Die Versorgungsspannung ist redundant anschließbar (9-36 VDC).

mGuard smart

Kleinste Geräteausführung. Kann z. B. einfach zwischen Rechner oder lokalem Netz (an LAN Port des mGuard) und einem vorhandenem Router (an WAN Port des mGuard) gesteckt werden, ohne dass beim bestehenden System Konfigurationsänderungen oder Treiberinstallationen erforderlich sind.
Konzipiert für den schnellen Einsatz im Büro oder unterwegs.

mGuard PCI



Diese in einem PCI-Steckplatz einsetzbare Karte bietet im *Treibermodus* dem Rechner, in dem die Karte installiert ist, alle mGuard-Funktionen und fungiert zusätzlich als normale Netzwerkkarte. Im *Power-over-PCI Modus* kann eine im Rechner bereits vorhandene Netzwerkkarte, oder aber ein anderer Rechner / Netz angeschlossen werden.

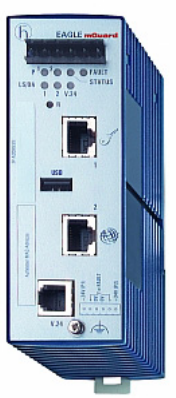
mGuard blade

Das mGuard bladePack besteht aus dem mGuard bladeBase, das problemlos in Standard 3 U Racks (19 Zoll) eingebaut werden kann und bis zu 12 mGuard blades zuzüglich einem Blade-Controller aufnimmt. Damit eignet sich diese Geräteausführung vor allem im industriellem Umfeld, um mehrere Server-Systeme individuell und unabhängig voneinander

ander schützen zu können. Eine zusätzliche serielle Schnittstelle ermöglicht Fernkonfiguration über eine Telefon-Wählverbindung oder ein Terminal.

EAGLE mGuard

Der EAGLE mGuard ist für die Montage auf Hutschienen (gemäß DIN EN 50 022) konzipiert und ist damit vor allem für den Einsatz im industriellem Umfeld geeignet. Der optionale Konfigurationsanschluss und die Option zur Herstellung einer Telefon-Wählverbindung über die V.24 Schnittstelle eröffnen zusätzliche Einsatzmöglichkeiten.



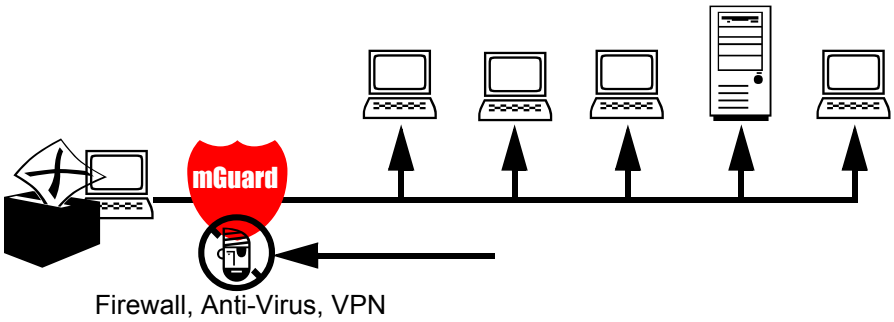
mGuard delta

Als kompakter LAN Switch (Ethernet / Fast Ethernet) ist diese Geräteausführung für den Anschluss von bis zu 4 LAN-Segmenten konzipiert. Damit eignet sich das Gerät besonders in logisch segmentierten Netzwerkumgebungen, bei denen sich die lokal angeschlossenen Rechner / Netze die mGuard-Funktionen teilen. Eine zusätzliche serielle Schnittstelle ermöglicht Konfiguration über eine Telefon-Wählverbindung oder ein Terminal. Mit seinem robusten Metallgehäuse ist der mGuard delta nicht nur als Desktop-Gerät sondern auch zur Unterbringung in Verteilerräumen geeignet.

2 Typische Anwendungsszenarien

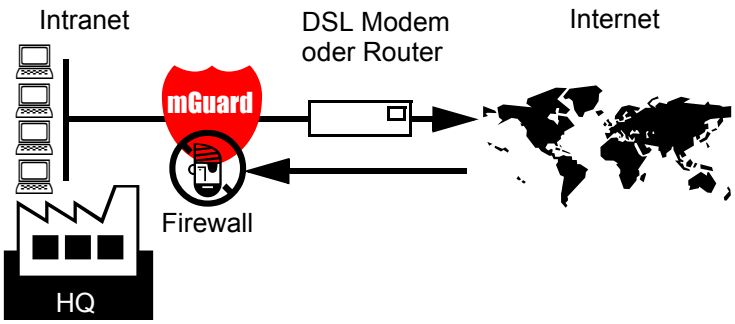
Nachfolgend werden verschiedene mögliche Anwendungsszenarien für den mGuard skizziert.

Stealth-Modus



Im *Stealth*-Modus (Werkseinstellung) kann der mGuard zwischen einen einzelnen Rechner und das übrige Netzwerk gesetzt werden.
Die Einstellungen für Firewall, Anti-Virus und VPN können mit einem Webbrowser unter der URL https://1.1.1.1/ vorgenommen werden.
Auf dem Rechner selbst müssen keine Konfigurationsänderungen durchgeführt werden.

Netzwerkrouter

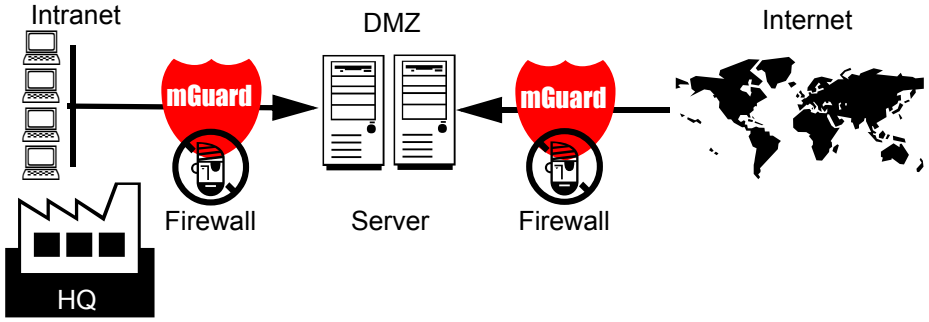


Der mGuard kann für mehrere Rechner als Netzwerkrouter die Internetanbindung bereitstellen und das Firmennetz dabei mit seiner Firewall schützen.
Dazu kann einer der folgenden Netzwerk-Modi des mGuard genutzt werden:

- *Router*, wenn der Internet-Anschluss z.B. über einen DSL-Router oder eine Standleitung erfolgt.
- *PPPoE*, wenn der Internet-Anschluss z.B. per DSL-Modem erfolgt und das PPPoE-Protokoll verwendet wird (z.B. in Deutschland).
- *PPTP*, wenn der Internet-Anschluss z. B. per DSL-Modem erfolgt und das PPTP-Protokoll verwendet wird (z. B. in Österreich).
- *Modem*, wenn der Internet-Anschluss über ein seriell angeschlossenes Modem (Hayes bzw. AT Befehlssatz kompatibel) erfolgt.

Bei Rechnern im Intranet muss der mGuard als Defaultgateway festgelegt sein.

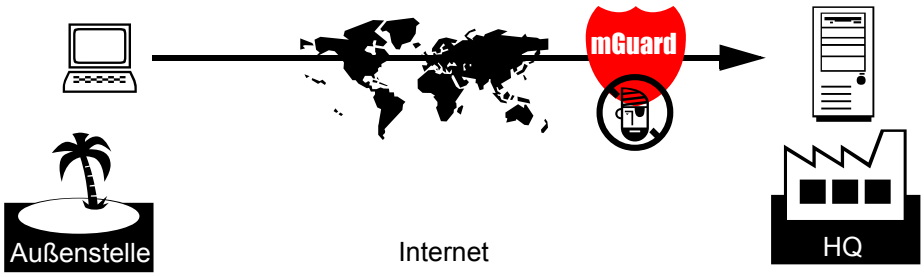
DMZ



Eine DMZ (Demilitarized Zone, deutsch: entmilitarisierte Zone) ist ein geschütztes Netzwerk, das zwischen zwei anderen Netzen liegt. Z.B. kann sich die Web-

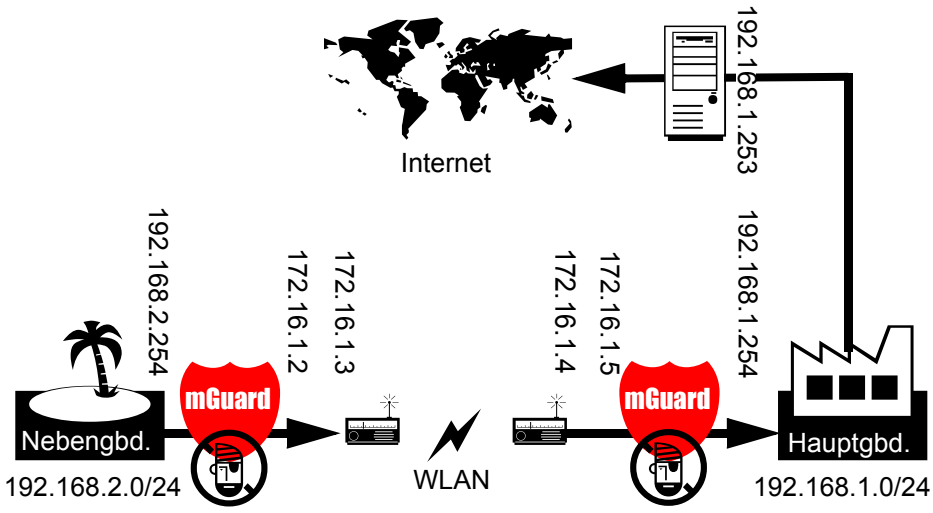
präsenz einer Firma so in der DMZ befinden, dass nur aus dem Intranet heraus mittels FTP neue Seiten auf den Server kopiert werden können, der lesende Zugriff per HTTP auf die Seiten jedoch auch aus dem Internet heraus möglich ist.
Die IP Adressen innerhalb der DMZ können öffentlich sein, oder aber privat, wobei der mit dem Internet verbundene mGuard die Verbindungen mittels Portforwarding an die privaten Adressen innerhalb der DMZ weiterleitet.

VPN Gateway



Mitarbeitern einer Firma soll ein verschlüsselter Zugang zum Firmennetz von zu Hause oder von unterwegs aus zur Verfügung gestellt werden. Der mGuard übernimmt dabei die Rolle des VPN Gateways.
Auf den externen Rechnern muss dazu eine IPsec fähige VPN-Client Software installiert werden, das Betriebssystem diese Funktionalität unterstützen, wie z.B. Windows 2000/XP, oder der Rechner mit einem mGuard ausgerüstet sein.

WLAN über VPN



Zwei Gebäude einer Firma sollen über eine mit IPsec geschützte WLAN Strecke miteinander verbunden werden. Vom Nebengebäude soll zudem der Internetzugang des Hauptgebäudes mitgenutzt werden können.

In diesem Beispiel wurden die mGuards in den *Router-M*odus geschaltet und für das WLAN ein eigenes Netz mit 172.16.1.x Adressen eingerichtet.
Da vom Nebengebäude aus das Internet über das VPN erreichbar sein soll, wird hier eine Default Route über das VPN eingerichtet:

Tunnelkonfiguration im Nebengebäude

Verbindungstyp	Tunnel (Netz <-> Netz)
Adresse des lokalen Netzes	192.168.2.0/24
Adresse des gegenüberliegenden Netzes	0.0.0.0/0

Im Hauptgebäude wird das entsprechende Gegenstück der Verbindung konfigu-

riert:

Tunnelkonfiguration im Hauptgebäude

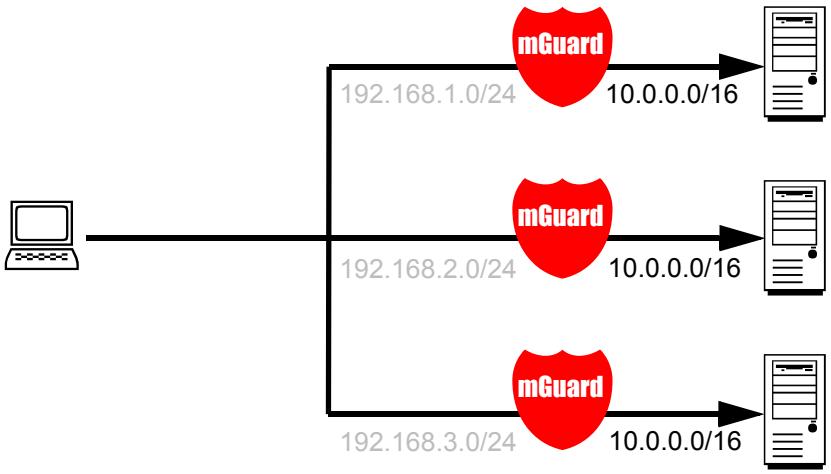
Verbindungstyp	Tunnel (Netz <-> Netz)
Lokales Netz	0.0.0.0
Adresse des gegenüberliegenden Netzes	192.168.2.0/24

Die Default Route eines mGuards führt normalerweise über den WAN Port. In diesem Fall jedoch ist das Internet über den LAN Port erreichbar:

Default Gateway im Hauptgebäude:

IP des Default Gateways	192.168.1.253

Auflösen von Netzwerkkonflikten

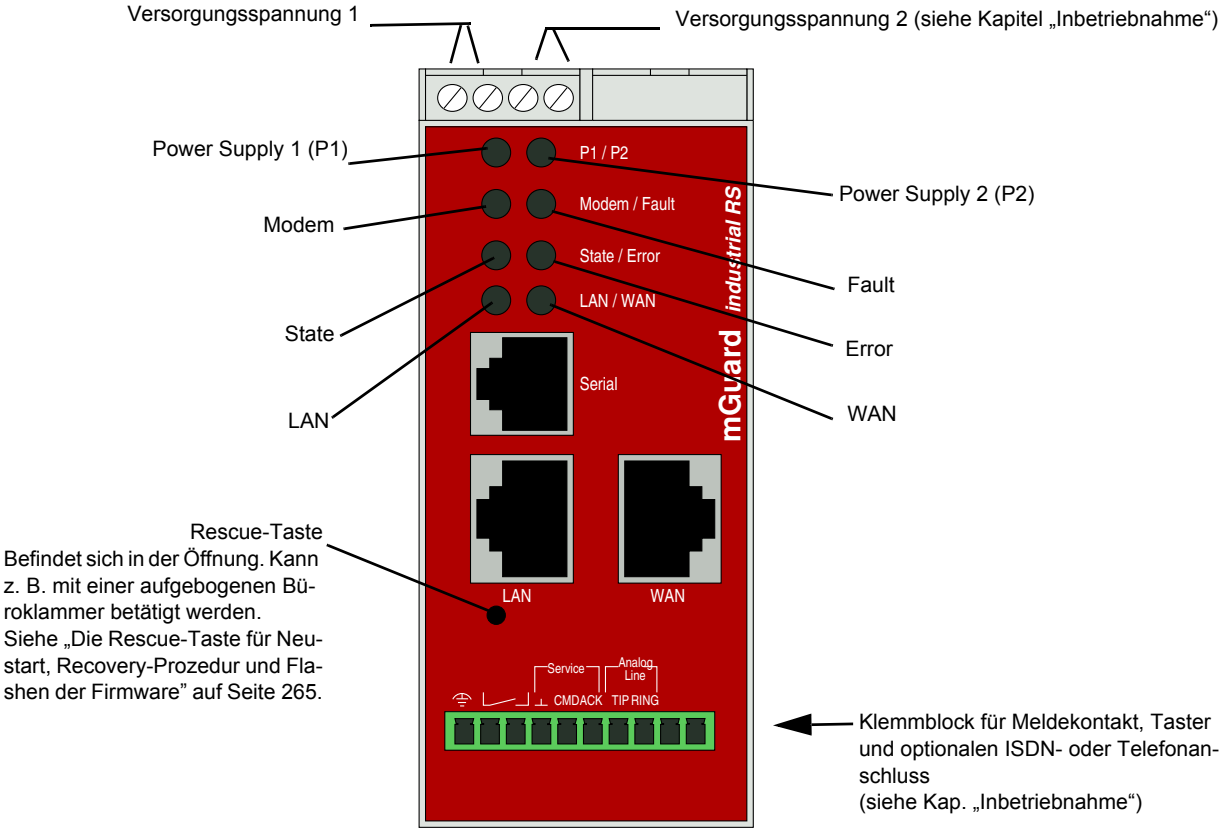


In der obigen Zeichnung sollen die Netzwerke auf der rechten Seite von dem Netzwerk oder Rechner auf der linken Seite erreichbar sein. Aus historischen oder technischen Gründen überschneiden sich jedoch die Netzwerke auf der rechten Seite.
Mit Hilfe der mGuards und ihrem 1:1 NAT Feature können diese Netze nun auf andere Netze umgeschrieben werden, so dass der Konflikt aufgelöst wird.

(1:1 NAT kann im normalen Routing und in IPsec Tunneln genutzt werden.)

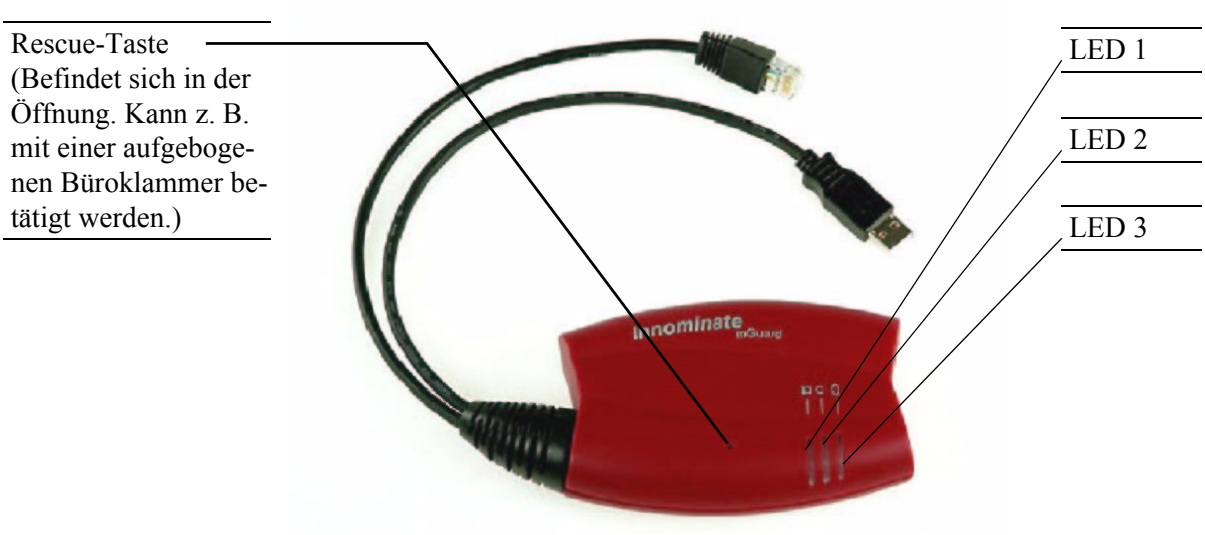
3 Bedienelemente und Anzeigen

3.1 mGuard industrial RS



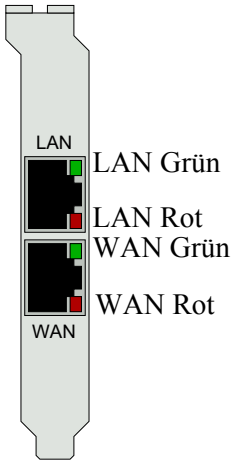
LED	Zustand	Bedeutung
P1	grün leuchtend	Stromversorgung 1 ist aktiv
P2	grün leuchtend	Stromversorgung 2 ist aktiv
Modem	grün leuchtend	Verbindung per Modem hergestellt
Fault	rot leuchtend	Der Meldekontakt ist aufgrund eines Fehlers offen - siehe „mGuard industrial RS installieren” auf Seite 24, unter „Meldekontakt“. (Während eines Neustarts ist der Meldekontakt unterbrochen.)
State	grün blinkend	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
Error	rot blinkend	**Systemfehler**. Führen Sie einen Neustart durch. ⌧ Dazu die Rescue-Taste kurz (1,5 Sek.) drücken ODER Das Gerät von der Stromversorgung kurz trennen und dann wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 265) oder wenden Sie sich an den Support.
State + Error	abwechselnd blinkend (grün-rot)	**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
LAN	grün leuchtend	**Ethernetstatus**. Zeigt den Status des LAN- bzw. WAN-Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
WAN	grün leuchtend	

3.2 mGuard smart



LEDs	Farbe	Zustand	Bedeutung
2	Rot/Grün	rot-grün blinkend	**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	Grün	blinkend	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
	Rot	blinkend	**Systemfehler**. ⌧ Führen Sie einen Neustart durch. Dazu die Recovery-Taste kurz (1,5 Sek.) drücken ODER Das Gerät von der Stromversorgung kurz trennen und dann wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 265) oder wenden Sie sich an den Support.
1 und **3**	Grün	leuchtend oder blinkend	**Ethernetstatus**. LED 1 zeigt den Status des LAN Ports, LED 3 den Status des WAN Ports. Sobald das Gerät am Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
1, 2, 3	div. LED-Leuchtcodes		**Recovery-Modus**. Nach Drücken der **Rescue**-Taste. Siehe „Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware” auf Seite 265.

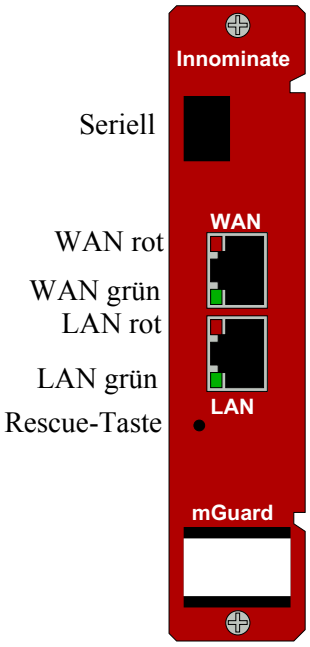
3.3 mGuard PCI



LEDs	Zustand	Bedeutung
WAN Rot, LAN Rot	blinkend	**Bootvorgang**. Nach dem Starten oder Neustarten des Rechners.
WAN Rot	blinkend	**Systemfehler**. ⌧ Führen Sie einen Neustart durch. Dazu die **Rescue**-Taste kurz (1,5 Sek.) drücken ODER Starten Sie den Computer neu. Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 265) oder wenden Sie sich an den Support.
WAN Grün, LAN Grün	leuchtend oder blinkend	**Ethernetstatus**. Zeigt den Status vom LAN bzw. WAN Interface. Sobald das Gerät angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
WAN Grün, WAN Rot, LAN Grün	div. LED-Leuchtcodes	**Recovery-Modus**. Nach Drücken der **Rescue**-Taste*****. Siehe „Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware” auf Seite 265

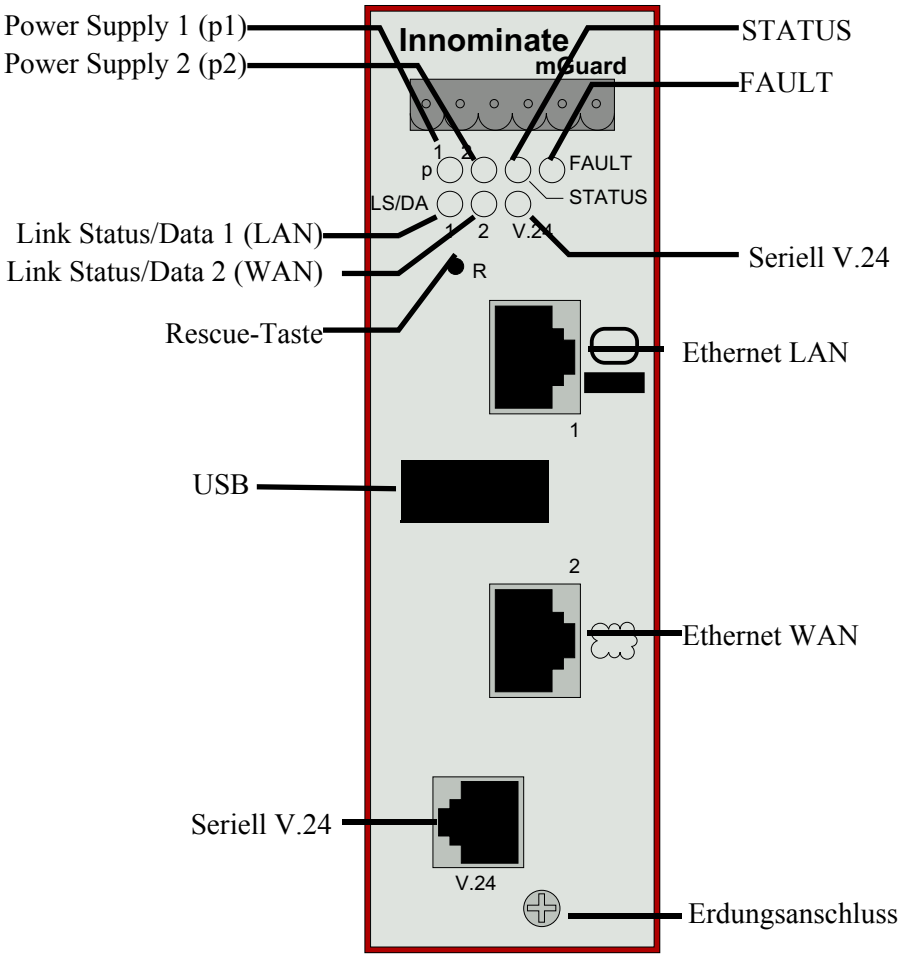
***** Beim mGuard PCI befindet sich die Rescue-Taste auf der Platine - siehe „Einbau der Hardware” auf Seite 40.

3.4 mGuard blade



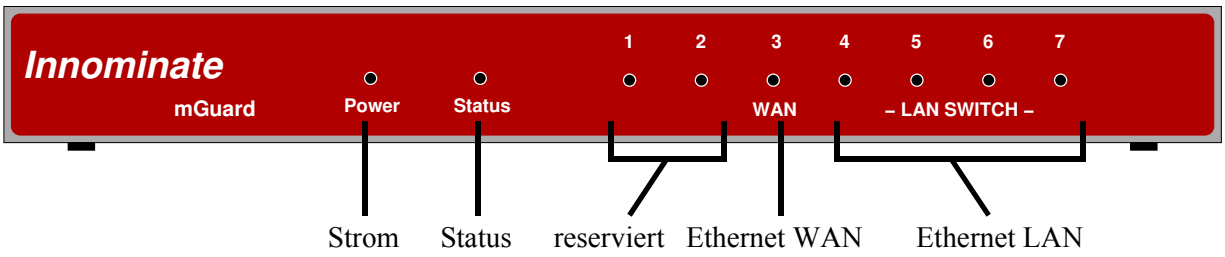
LEDs	Zustand	Bedeutung
WAN Rot, LAN Rot	blinkend	**Bootvorgang**. Nach dem Starten oder Neustarten des Rechners.
WAN Rot	blinkend	**Systemfehler**. ⌦ Führen Sie einen Neustart durch. Dazu die **Rescue**-Taste kurz (1,5 Sek.) drücken Falls der Fehler weiterhin auftritt, starten Sie die *Recovery-Prozedur* (siehe „Recovery-Prozedur ausführen” auf Seite 265) oder wenden Sie sich an den Support.
WAN Grün, LAN Grün	leuchtend oder blinkend	**Ethernetstatus**. Zeigt den Status vom LAN bzw. WAN Interface. Sobald das Gerät angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner besteht. Bei der Übertragung von Datenpaketen erlischt kurzzeitig die LED.
WAN Grün, WAN Rot, LAN Grün	div. LED-Leuchtcodes	**Recovery-Modus**. Nach Drücken der **Rescue**-Taste. Siehe „Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware” auf Seite 265

3.5 EAGLE mGuard



LEDs	Zustand	Bedeutung
p1, p2	grün leuchtend	Die Stromversorgung 1 bzw. 2 ist aktiv.
STATUS	grün blinkend	Der mGuard bootet.
	grün leuchtend	Der mGuard ist bereit.
	gelb leuchtend	Der mGuard ist bereit und Redundancy Master.
	gelb/grün blinkend	Der mGuard ist bereit und Redundancy Slave.
FAULT	rot	Der Meldekontakt ist infolge eines Fehlers offen. Siehe „EAGLE mGuard installieren” auf Seite 33, unter „Meldekontakt“.
LS/DA 1/2 V.24	grün	Link vorhanden
	gelb blinkend	Datentransfer

3.6 mGuard delta



LEDs	Zustand	Bedeutung
Power	ein	Die Stromversorgung ist aktiv.
Status	ein	Der mGuard startet.
	Heartbeat (aufleuchten, aufleuchten, Pause, ...)	Der mGuard ist bereit.
1,2	-	Reserviert
3 (WAN)	ein	Link vorhanden
	blinkend	Datentransfer
4-7 (LAN)	ein	Link vorhanden
	blinkend	Datentransfer

4 Inbetriebnahme

Sicherheits-hinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss der mGuard richtig installiert, betrieben und gewartet werden. Bitte verwenden Sie den mGuard ausschließlich auf die dafür vorgesehene Art und für geeignete Zwecke.

Schließen Sie die Netzwerk-Ports des mGuard nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuard verbunden werden.

Warnung:

! Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

Bitte beachten Sie auch die weiteren gerätespezifischen Sicherheitshinweise in den folgenden Abschnitten.

Allgemeine Hinweise zur Benutzung

- mGuard PCI: Ihr PC muss einen freien PCI Slot (3,3V oder 5V) bereitstellen.
- Zum Reinigen des Gerätegehäuses ein weiches Tuch verwenden. Kein aggressives Lösungsmittel auftragen!
- Umgebungsbedingungen:
  0 bis +40°C (smart, blade, delta), 70°C (PCI), 55°C (mGuard industrial RS, EAGLE mGuard)
- max. Luftfeuchtigkeit 90% (mGuard industrial RS, EAGLE mGuard: 95%), nicht kondensierend
- Nicht direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aussetzen, um Überhitzung zu vermeiden.
- Anschlusskabel nicht knicken. Den Netzwerkstecker nur zum Verbinden mit einem Netzwerk benutzen.

Schritte zur Inbetriebnahme

Um das Gerät in Betrieb zu nehmen, führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

Schritt	Ziel	Seite
1	Lieferumfang prüfen, Release Notes lesen	„Zum Lieferumfang gehören” auf Seite 23
2	Gerät anschließen	„mGuard industrial RS installieren” auf Seite 24 „mGuard smart anschließen” auf Seite 30 „mGuard blade installieren” auf Seite 31 „EAGLE mGuard installieren” auf Seite 33 „mGuard delta anschließen” auf Seite 36 „mGuard PCI installieren” auf Seite 37
3	Das Gerät konfigurieren, soweit erforderlich. Gehen Sie dazu die einzelnen Menüoptionen durch, die Ihnen der mGuard mit seiner Konfigurationsoberfläche bietet. Lesen Sie deren Erläuterungen in diesem Handbuch, um zu entscheiden, welche Einstellungen für Ihre Betriebsumgebung erforderlich oder gewünscht sind.	„Lokale Konfiguration: Bei Inbetriebnahme” auf Seite 48

Zum Lieferumfang gehören

Prüfen Sie vor Inbetriebnahme die Lieferung auf Vollständigkeit:

- Das Gerät *mGuard industrial RS*, *mGuard blade, delta, PCI, smart* oder *EAGLE mGuard*
- Quick Installation Guide

Zum mGuard industrial RS gehören zusätzlich:

- Klemmblock für den Stromanschluss (aufgesteckt)
- Klemmblock für den Meldekontakt, Taster sowie optionalen ISDN- oder Telefonanschluss

Zum mGuard bladePack gehören zusätzlich:

- Die 19'' mGuard bladeBase
- 1 mGuard blade als Kontroller
- 2 Netzteile
- 2 Netzkabel
- 12 Leerblenden
- 12 Beschriftungsplätchen M1 bis M12
- Schrauben zur Montage der bladeBase

Zum mGuard delta gehören zusätzlich:

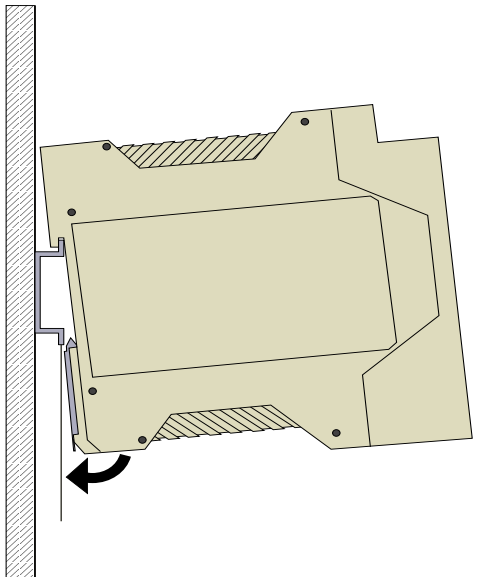
- eine 5V DC Stromversorgung
- zwei UTP Ethernetkabel

4.1 mGuard industrial RS installieren

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für die Montage und die Vornahme der Anschlüsse ist folgender Ablauf zweckmäßig:

1. Ziehen Sie den Klemmblock unten vom mGuard industrial RS ab und verdrahten Sie die Meldeleitungen und die weiteren Anschlüsse, soweit vorhanden bzw. soweit sie verwendet werden - siehe unten unter „Anschlussmöglichkeiten Klemmblock unten” auf Seite 26.
   Die Schrauben der Schraubklemmen mit mindestens 0,22 Nm anziehen.
   Verdrahteten Klemmblock nach der Montage des Gerätes auf der Hutschiene wieder aufsetzen.
2. Montieren Sie den mGuard industrial RS auf einer 35 mm Hutschiene nach DIN EN 50 022.
   Hängen Sie dazu die obere Rastführung des mGuard industrial RS in die Hutschiene ein und drücken Sie den mGuard industrial RS dann nach unten gegen die Hutschiene, so dass er einrastet.



3. Am Klemmblock oben die Versorgungsspannung anschließen - siehe unten unter „Versorgungsspannung” auf Seite 25.
4. Am LAN-Port bzw. WAN-Port die erforderlichen Netzwerkanschlüsse vornehmen - siehe unten unter „Netzwerkverbindung” auf Seite 25.
5. Gegebenenfalls am SERIAL-Port das entsprechende Gerät anschließen - siehe unten unter „Serial-Port” auf Seite 29.

⌧ Das Gerät leitet die per Hutschiene gelieferte Erdung durch zum linken Kontakt (Erdungsanschluss) der unteren Klemmleiste.

⌧ Das Gehäuse darf nicht geöffnet werden.

⌧ Die Schirmungsmasse der anschließbaren Twisted Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

Warnung:
Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu treffen. Der Innominate mGuard industrial RS darf bei Aufstellung in Wohn- und Büroumgebungen ausschließlich in Schaltschränken mit Brandschutzeigenschaften gemäß EN 60950-1 betrieben werden.

Demontage

Anschlüsse abnehmen bzw. trennen.

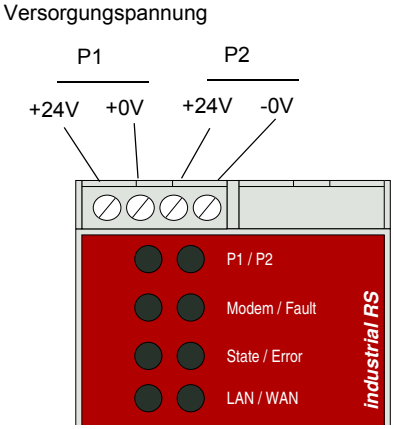
Um den mGuard industrial RS von der Hutschiene zu demontieren, stecken Sie

einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen den mGuard industrial RS nach oben.

Anschlüsse

Versorgungsspannung

Der Anschluss der **Versorgungsspannung** erfolgt über einen Klemmblock mit Schraubverriegelung, der sich oben auf dem Gerät befindet.



Sicherheitshinweis: Der Innominate mGuard industrial RS ist für den Betrieb an einer Gleichspannung von 9 - 36V DC/SELV max. 0,5A vorgesehen. Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschlossen werden.

Betriebsspannung

NEC Class 2 power source 12VDC bzw. 24VDC -25% +33% Sicherheitskleinspannung (SELV/PELV, redundante Eingänge entkoppelt), max. 5A. Pufferzeit min. 10ms bei 24VDC.

Redundante Spannungsversorgung

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den mGuard industrial RS alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

⌧ Bei nicht redundanter Zuführung der Versorgungsspannung meldet der mGuard industrial RS über den Meldekontakt (s. u.) den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen.

Netzwerkverbindung

Sicherheitshinweis: Schließen Sie die Netzwerk-Ports des mGuard nur an LAN-Installationen an. Zum Aufbau von Netzwerkverbindungen sind Kabel mit Knickschutzhülle an den Steckern zu verwenden. Unbenutzte Buchsen sind mit den mitgelieferten Staubschutzkappen abzudecken. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuard verbunden werden.

LAN-Port:

Verbinden Sie den lokalen Rechner oder das lokale Netzwerk mittels eines UTP Ethernetkabels (CAT 5) mit dem LAN-Port des mGuard.
Ist Ihr Rechner bereits an einem Netzwerk angeschlossen, dann patchen Sie den mGuard *zwischen* die bereits bestehende Netzwerkverbindung.

Beachten Sie bitte, dass die Konfiguration zunächst nur über das LAN Interface erfolgen kann und die Firewall des mGuard industrial RS den gesamten IP Datenverkehr vom WAN zum LAN Interface unterbindet.

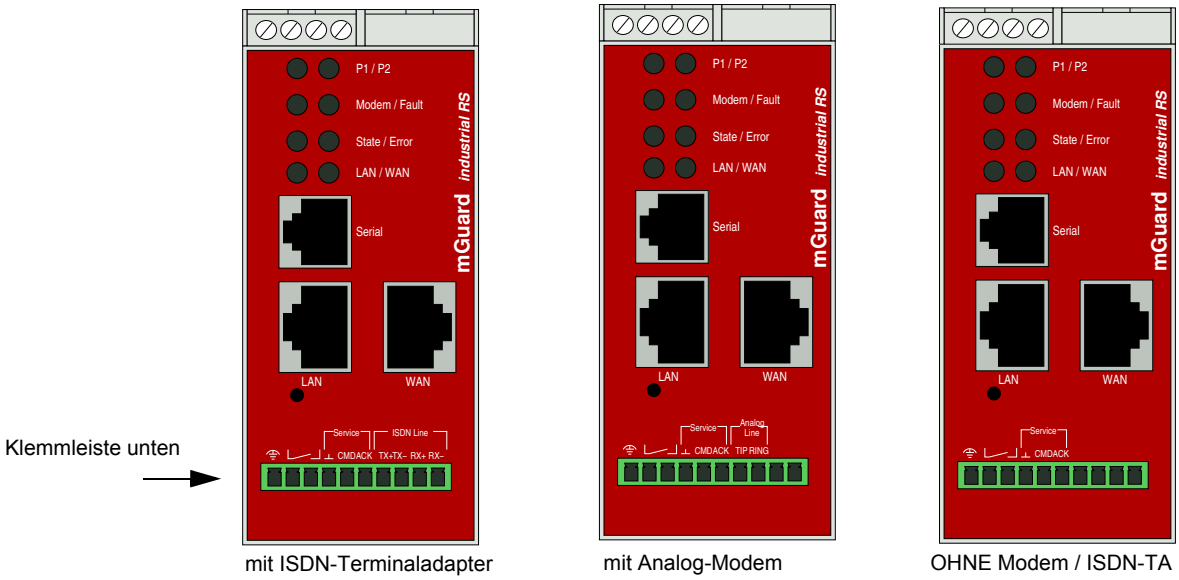
WAN Port:

Buchse zum Anschließen an das externe Netzwerk, z. B. WAN, Internet. (Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.) Benutzen Sie ein UTP-Kabel (CAT 5).

- Es ist keine Treiber-Installation erforderlich.
- Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.

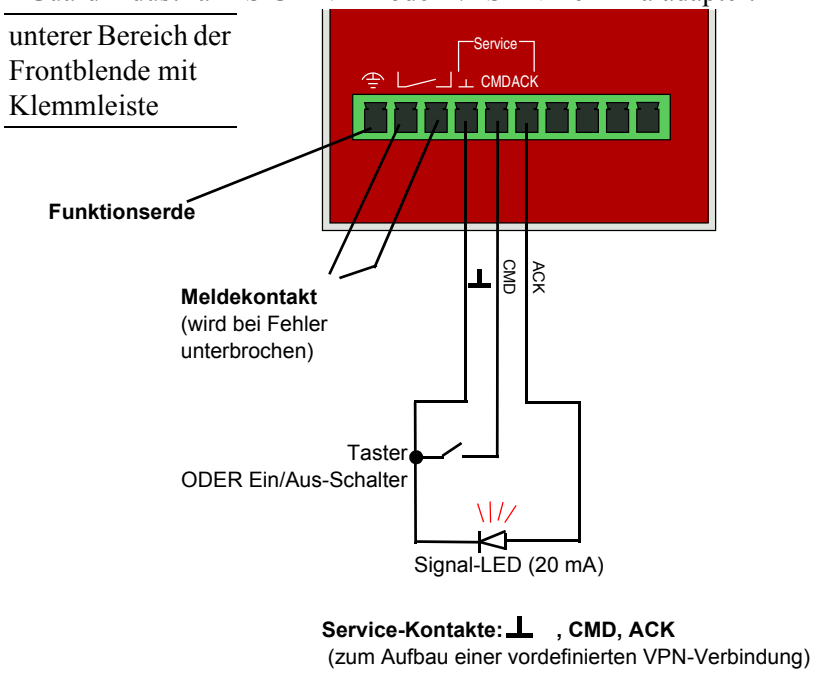
Anschlussmöglichkeiten Klemmblock unten

Der mGuard industrial RS ist in drei Versionen lieferbar, äußerlich unterscheidbar anhand der Anschlussmöglichkeiten bei der Klemmleiste unten:



mit ISDN-Terminaladapter | mit Analog-Modem | OHNE Modem / ISDN-TA

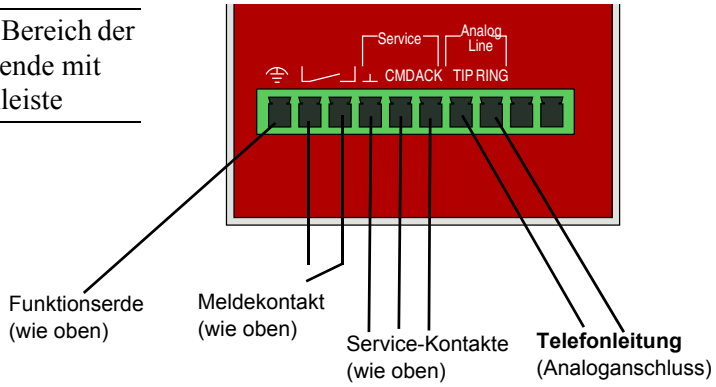
mGuard industrial RS **OHNE** Modem / ISDN-Terminaladapter:



Service-Kontakte: ⊥ , CMD, ACK
(zum Aufbau einer vordefinierten VPN-Verbindung)

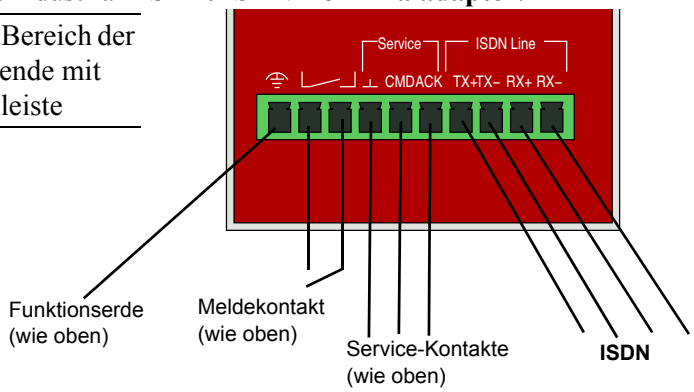
mGuard industrial RS **mit Modem**:

unterer Bereich der Frontblende mit Klemmleiste



mGuard industrial RS **mit ISDN-Terminaladapter**:

unterer Bereich der Frontblende mit Klemmleiste



Funktionserde

Kann für Zwecke des Benutzers verwendet werden. Dieser Anschluss ist leitend mit der Rückseite des mGuard industrial RS verbunden. Die Erdung des mGuard industrial RS erfolgt bei Montage auf einer Hutschiene mit der Metallklemme, über die er über seine Rückseite mit der Hutschiene verbunden ist. Die Hutschiene muss geerdet sein.

Meldekontakt

Sicherheitshinweis: An den Meldekontakt dürfen nur SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschlossen werden.

Der Meldekontakt dient der Funktionsüberwachung des mGuard industrial RS und ermöglicht damit eine Ferndiagnose. Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung folgendes gemeldet:

– Der Ausfall mindestens einer der zwei Versorgungsspannungen.
– Eine Grenzwertunterschreitung bei der Stromversorgung des mGuard industrial RS (Versorgungsspannung 1 und/oder 2 ist kleiner als 9 V).
– Der fehlerhafte Linkstatus mindestens eines Ports. Die Meldung des Linkstatus kann beim mGuard industrial RS pro Port über das Management maskiert werden.
  Im Lieferzustand erfolgt keine Verbindungsüberwachung.
– Fehler beim Selbsttest.

⌧ Während eines Neustarts ist der Meldekontakt unterbrochen, bis der mGuard vollständig den Betrieb aufgenommen hat. Das gilt auch, wenn der Meldekontakt per Software-Konfiguration manuell auf *Geschlossen* gestellt ist.

Service-Kontakte

Sicherheitshinweis: Die Service-Kontakte (⏚, CMD, ACK) dürfen an keine externe Spanungsquelle angeschlossen werden, sondern sind wie hier beschrieben zu verbinden.

Zwischen die Service-Kontakte CMD und ⏚ kann ein Taster oder ein Ein/Aus-Schalter (z. B. Schlüsselschalter) angeschlossen werden. Zwischen den Kontakten ACK (+) und ⏚ (-) kann eine handelsübliche LED (bis 3,5 V) oder ein entsprechender Optokoppler angeschlossen werden. Der Kontakt ist kurzschlußfest und liefert maximal 20 mA. Die LED beziehungsweise der Optokoppler muß ohne Vorwiderstand angeschlossen werden. Für die Verdrahtung siehe Grafik oben. Der Taster oder Ein/Aus-Schalter dient zum Aufbau und Abbau einer zuvor definierten VPN-Verbindung, und die LED signalisiert den Status der VPN-Verbindung.
Siehe „IPsec VPN » Global” auf Seite 206 unter **Optionen**.

Bedienung eines angeschlossenen Tasters:

Zum Aufbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis die Signal-LED blinkt. Erst dann den Taster loslassen. Das Blinken signalisiert, dass der mGuard das Kommando zum Aufbau der VPN-Verbindung erhalten hat und dabei ist, die VPN-Verbindung aufzubauen. Sobald die VPN-Verbindung steht, leuchtet die Signal-LED kontinuierlich.

Zum Abbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis die Signal-LED blinkt oder erlischt. Erst dann den Taster loslassen.

Sobald die Signal-LED nicht mehr leuchtet, ist die VPN-Verbindung abgebaut.

Bedienung eines angeschlossenen Ein/Aus-Schalters:

Zum Aufbau der VPN-Verbindung den Schalter auf EIN stellen.

Zum Abbau der VPN-Verbindung den Schalter auf AUS stellen.

Signal-LED: Ist die Signal-LED auf AUS, wird dadurch generell signalisiert, dass die definierte VPN-Verbindung nicht besteht. Ursache: VPN-Verbindung nicht aufgebaut oder ausgefallen wegen Fehler. Ist die Signal-LED auf EIN, besteht die VPN-Verbindung. Blinkt die Signal-LED, wird die VPN-Verbindung gerade auf- oder abgebaut.

Analog Line (bei integriertem Modem)

Sicherheitshinweis: Die analogen Anschlüsse (TIP, RING) dürfen nur an die dafür vorgesehene Fernmeldeleitung angeschlossen werden.

Die Kontakte TIP und RING sind für den Anschluss ans Telefon-Festnetz (Analoganschluss).
Für die auf der Frontblende angegebenen Kontaktbezeichnungen sind in Deutschland auch folgende Bezeichnungen gebräuchlich:

TIP = a	RING = b

ISDN Line (bei integriertem ISDN-Terminaladapter)

Sicherheitshinweis: Die ISDN Anschlüsse (TX+, TX-, RX+, RX-) dürfen nur an einen ISDN S0 Bus angeschlossen werden.

Die Kontakte TX+, TX-, RX+ und RX– sind für den Anschluss ans ISDN und bezeichnen den mGuard industrial RS als Teilnehmer am ISDN. Die folgende

Tabelle beschreibt die Zuordnung der Kontakte zu 8-poligen Verbindungen sowohl für Stecker als auch Dosen, zum Beispiel RJ45:

Pol Nummer	TE (mGuard)
3	TX+
4	RX+
5	RX-
6	TX-

Serial-Port

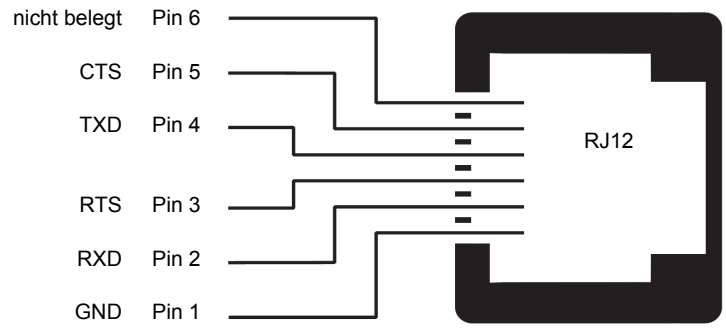
Sicherheitshinweis: Die serielle Schnittstelle (RJ12-Buchse) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit RJ12-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30m.

Der Serial-Port (serielle Schnittstelle) kann wie folgt verwendet werden:

a) Zum Konfigurieren des mGuard über die serielle Schnittstelle. Dazu gibt es zwei Möglichkeiten:
An die serielle Schnittstelle des mGuard wird direkt ein PC angeschlossen (über dessen serielle Schnittstelle). Dann kann der PC-Benutzer mittels eines Terminalprogramms über die Kommandozeile den mGuard konfigurieren.
Oder an die serielle Schnittstelle des mGuards wird ein Modem angeschlossen, das am Telefonnetz (Festnetz oder GSM-Netz) angeschlossen ist. Dann kann der Benutzer eines entfernten PCs, der ebenfalls mit einem Modem am Telefonnetz angeschlossen ist, zum mGuard eine PPP-Wählverbindung (PPP = Point-to-Point Protocol) herstellen und ihn per Web-Browser konfigurieren.

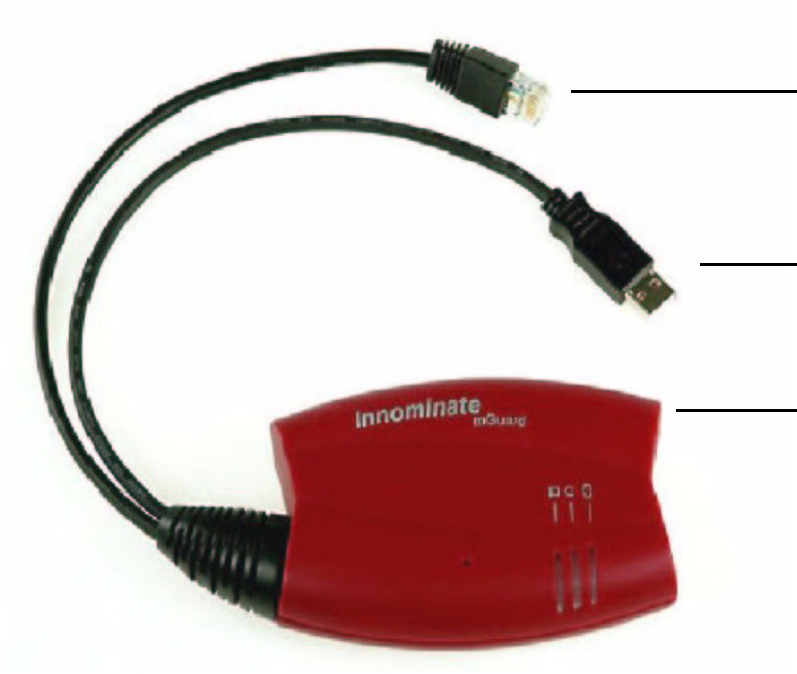
b) Zur Abwicklung des Datenverkehrs statt über die WAN-Schnittstelle des mGuard über die serielle Schnittstelle. In diesem Fall ist an die serielle Schnittstelle ein Modem anzuschließen.

Pin-Belegung der RJ12-Buchse (Serial Port)



Beim mGuard industrial RS mit eingebautem Modem oder ISDN-Terminaladapter kann der Datenverkehr statt über die WAN-Schnittstelle über die Anschlüsse *Analog Line* bzw. *ISDN Line* erfolgen.

4.2 mGuard smart anschließen



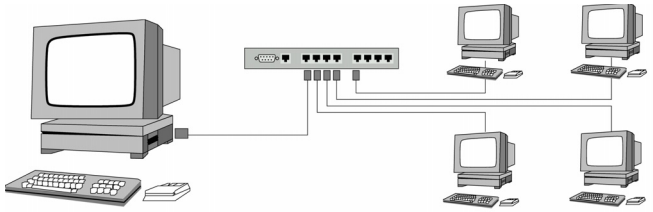
LAN Port: Ethernet-Stecker zum direkten Anschließen an das zu schützende Gerät bzw. Netz (**lokales** Gerät oder Netz).

USB-Stecker zum Anschließen an die USB-Schnittstelle eines Rechners.
Dient nur zur Stromversorgung!

WAN Port: Buchse zum Anschließen an das externe Netzwerk, z. B. WAN, Internet.
(Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)
Benutzen Sie ein UTP-Kabel (CAT 5).

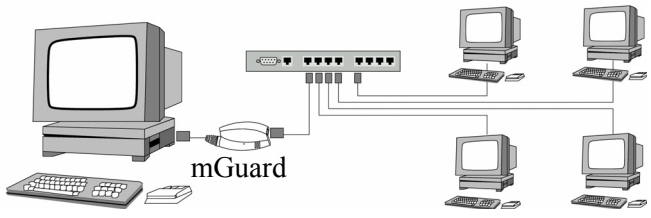
Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann stekken Sie den mGuard zwischen die Netzwerkschnittstelle des Rechners (= dessen Netzwerkkarte) und das Netzwerk.

vorher:



nachher:

(Links kann auch ein LAN sein.)

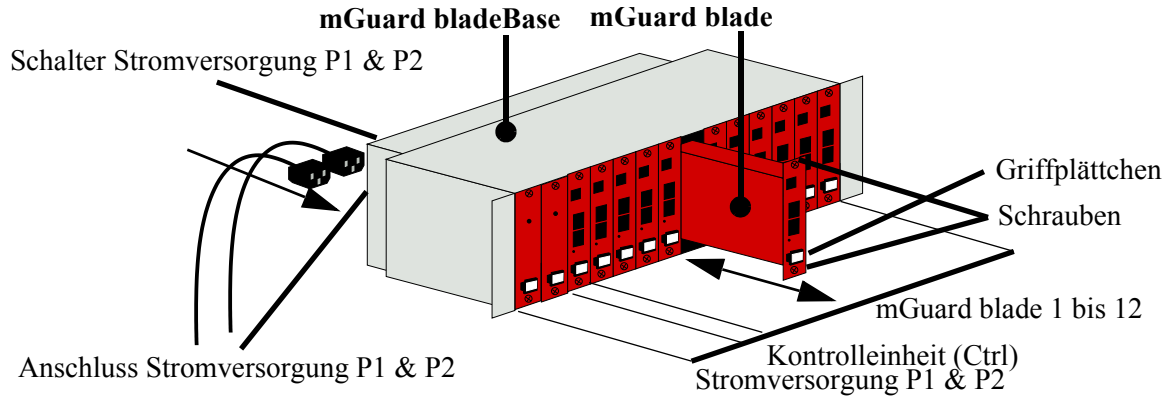


⌦ Es ist keine Treiber-Installation erforderlich.

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.

Warnung:
Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu treffen.

4.3 mGuard blade installieren



mGuard bladeBase installieren

- Bauen Sie die mGuard bladeBase in das Rack ein, z.B. in der Nähe des Patchfeldes.
- Versehen Sie die beiden Stromversorgungen und die Kontrolleinheit an der Vorderseite von links nach rechts mit den Griffplättchen „P1“, „P2“ und „Ctrl“.
- Verbinden Sie die beiden Stromversorgungen auf der Rückseite der mGuard bladeBase mit 100V oder 220/240V.
- Schalten Sie die beiden Stromversorgungen ein.
- Die LEDs an der Vorderseite der Stromversorgungen leuchten nun grün.

⌦ **Unbedingt darauf achten, dass eine ausreichende Luftzirkulation für das BladePack sichergestellt ist!**

⌦ **Bei Stapelung von mehreren BladePacks müssen ein oder mehrere Zoll Lüftereinschübe vorgesehen werden, damit die aufgestaute Warmluft abgeführt werden kann!**

mGuard blade installieren

- Lösen Sie an der Blende bzw. am zu ersetzenden mGuard blade die obere und untere Schraube.
- Nehmen Sie die Blende ab bzw. ziehen Sie das alte mGuard blade heraus.
- Setzen Sie das neue mGuard blade mit der Leiterplatte in die Kunststoffführungen und schieben Sie es vollständig in das mGuard bladeBase hinein.
- Sichern Sie das mGuard blade durch leichtes Anziehen der Schrauben.
- Ersetzen Sie das leere Griffplättchen durch das mit der passenden Nummer aus dem Zubehör der mGuard bladeBase, oder ersetzen Sie es durch das des ausgetauschten mGuard blade. Dazu das Plättchen seitlich hinein- bzw. herausschieben.

⌦ Die mGuard bladeBase braucht beim Ein- und Ausbau eines mGuard blade nicht ausgeschaltet zu werden.

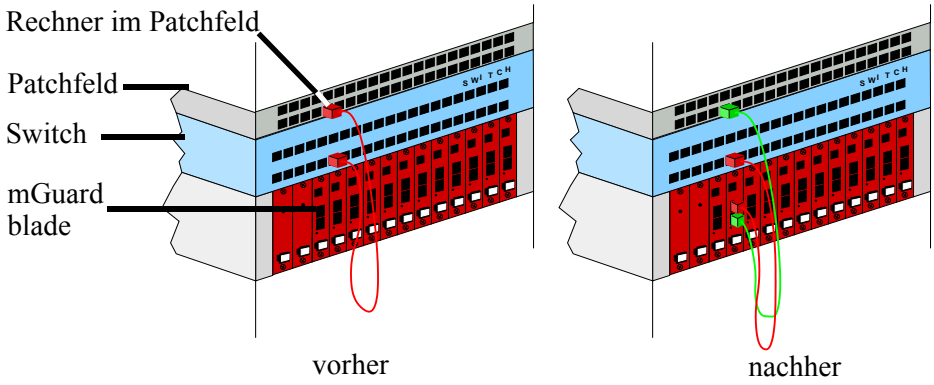
Kontrolleinheit (CTRL Slot)

Direkt neben den beiden Stromversorgungen befindet sich der „CTRL“ Slot. Ein darin betriebener mGuard blade arbeitet als Kontroller für alle anderen mGuard blades.

Bei der ersten Installation eines mGuard blade in den „CTRL“ Slot konfiguriert sich das blade in eine Kontrolleinheit wie folgt um:

- Die Benutzeroberfläche wird für den Betrieb als Kontroller umkonfiguriert.
- Er schaltet sich in den Router-Modus mit der lokalen IP 192.168.1.1.
- Die Funktionen Firewall, Anti-Virus und VPN werden zurückgesetzt und deaktiviert.

Anschluss mGuard blade



Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann patchen Sie das mGuard blade zwischen die bereits bestehende Netzwerkverbindung.

Beachten Sie bitte, dass die Konfiguration zunächst nur vom lokalen Rechner aus über das LAN Interface erfolgen kann und die Firewall des mGuard allen IP Datenverkehr vom WAN zum LAN Interface unterbindet.

- Es ist keine Treiber-Installation erforderlich.
- Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.

Serial-Port

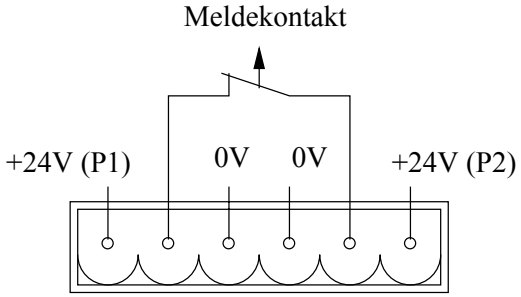
Sicherheitshinweis: Die serielle Schnittstelle (RJ12-Buchse) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit RJ12-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30m.

Der Serial-Port (serielle Schnittstelle) kann so benutzt werden, wie es unter „Serial-Port” auf Seite 29 beschrieben ist.

4.4 EAGLE mGuard installieren

Klemmblock

Der Anschluss der **Versorgungsspannung** und des **Meldekontaktes** erfolgt über einen 6-poligen Klemmblock.



Sicherheitshinweis: Der EAGLE mGuard ist für den Betrieb mit Sicherheitskleinspannung ausgelegt. Entsprechend dürfen an die Versorgungsspannungsanschlüsse sowie an den Meldekontakt nur PELV-Spannungskreise oder wahlweise SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschossen werden.

Der EAGLE mGuard kann an einer Gleichspannung von 9,6 - 60V DC max. 1A beziehungsweise an einer Wechselspannung von 18 - 30V AC max. 1A betrieben werden. Verwenden Sie die Pins +24V und 0V zum Anschluß einer Wechselspannung.

Betriebsspannung

NEC Class 2 power source 12VDC bzw. 24VDC -25% +33% Sicherheitskleinspannung (SELV/PELV, redundante Eingänge entkoppelt), max. 5A. Pufferzeit min. 10ms bei 24VDC.

Redundante Spannungsversorgung

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den EAGLE mGuard alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Meldekontakt

Sicherheitshinweis: Der Meldekontakt darf nur an PELV-Spannungskreise oder wahlweise SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschlossen werden.

Der Meldekontakt dient der Funktionsüberwachung des EAGLE mGuard und ermöglicht damit eine Ferndiagnose. Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung folgendes gemeldet:

- Der Ausfall mindestens einer der zwei Versorgungsspannungen.
- Eine dauerhafte Störung im EAGLE mGuard (interne 3,3 VDC-Spannung, Versorgungsspannung 1 oder 2 < 9,6 V, …).
- Der fehlerhafte Linkstatus mindestens eines Ports. Die Meldung des Linkstatus kann beim EAGLE mGuard pro Port über das Management maskiert werden.
  Im Lieferzustand erfolgt keine Verbindungsüberwachung.
- Fehler beim Selbsttest.

⌦ Bei nicht redundanter Zuführung der Versorgungsspannung meldet der EAGLE mGuard den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen.

Erdungsanschluss

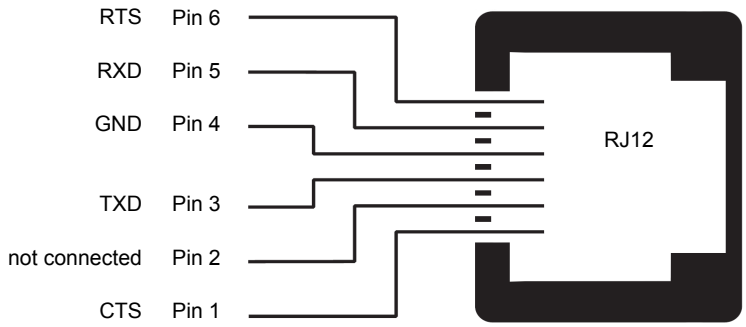
Zur Erdung des EAGLE mGuard ist ein separater Schraubanschluss vorhanden.

Serial-Port

Sicherheitshinweis: Die serielle Schnittstelle (RJ12-Buchse) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit RJ12-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30m.

Der Serial-Port (serielle Schnittstelle) kann so benutzt werden, wie es unter „Serial-Port" auf Seite 29 beschrieben ist. Doch die Belegung der Kontakte ist unterschiedlich wie es die folgende Abbildung zeigt:

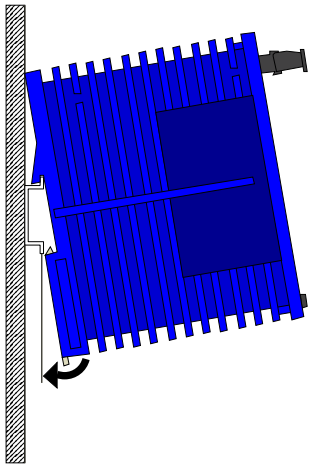
Pin-Belegung der RJ12-Buchse (Serial Port)



Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für die Montage ist folgender Ablauf zweckmäßig:

- Ziehen Sie den Klemmblock vom EAGLE mGuard ab, und verdrahten Sie die Versorgungsspannungs- und Meldeleitungen.
- Montieren Sie den EAGLE mGuard auf einer 35 mm Hutschiene nach DIN EN 50 022.
- Hängen Sie die obere Rastführung des EAGLE mGuard in die Hutschiene ein und drücken Sie den EAGLE mGuard dann nach unten gegen die Hutschiene, so dass er einrastet.
- Schließen Sie das Gerät an das lokale Netz oder den lokalen Rechner an, das/der geschützt werden soll (LAN).
- Über die Buchse zum Anschließen an das externe Netzwerk (WAN) den Anschluss ans externe Netzwerk vornehmen, z. B. Internet. (Über dieses Netzwerk werden die Verbindungen zum entfernten Gerät bzw. entfernten Netz hergestellt.)



☒ Die Erdung der Frontblende des Gehäuses des EAGLE mGuard erfolgt über

den Erdungsanschluss.

- Das Gehäuse darf nicht geöffnet werden.
- Die Schirmungsmasse der anschließbaren Industrial Twisted Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

Warnung:
Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu treffen. Der EAGLE mGuard darf bei Aufstellung in Wohn- und Büroumgebungen ausschließlich in Schaltschränken mit Brandschutzeigenschaften gemäß EN 60950-1 betrieben werden.

Inbetriebnahme

Mit dem Anschluss der Versorgungsspannung über den 6-poligen Klemmblock nehmen Sie den EAGLE mGuard in Betrieb. Verriegeln Sie den Klemmblock mit der seitlichen Verriegelungsschraube.

Netzwerkverbindung

Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann patchen Sie den EAGLE mGuard *zwischen* die bereits bestehende Netzwerkverbindung.

Beachten Sie bitte, dass die Konfiguration zunächst nur über das LAN Interface erfolgen kann und die Firewall des EAGLE mGuard den gesamten IP Datenverkehr vom WAN zum LAN Interface unterbindet.

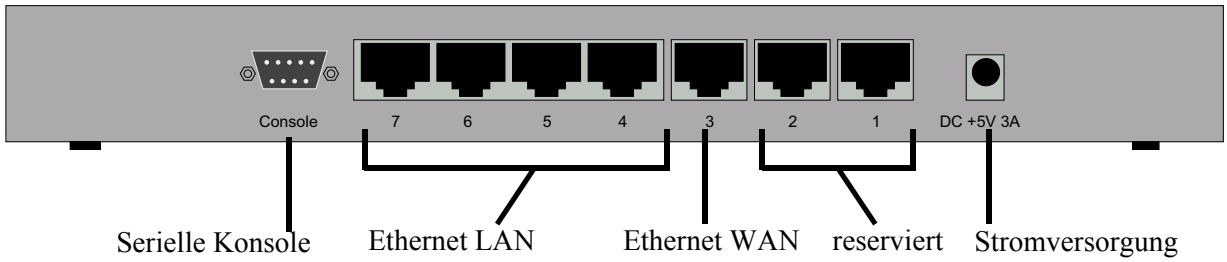
- Es ist keine Treiber-Installation erforderlich.
- Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern.
- Beide Netzwerkschnittstellen des EAGLE mGuard sind für den Anschluss an einen Rechner konfiguriert. Beim Anschluss an einen Hub ist Folgendes zu beachten: Bei deaktivierter *Autonegotiation* Funktion wird auch die Auto-MDIX Funktion deaktiviert, d.h. der Port des EAGLE mGuard muss entweder an den Uplink-Port des Hub oder mittels eines Cross-Link-Kabels mit dem Hub verbunden werden.

Demontage

Um den EAGLE mGuard von der Hutschiene zu demontieren, fahren Sie mit einem Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen den EAGLE mGuard nach oben.

4.5 mGuard delta anschließen

Sicherheitshinweis: Die serielle Schnittstelle (DE-9 Steckverbindung) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit einer DE-9 Steckverbinder zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30m.



- Verbinden Sie die Stromversorgung (5V DC, 3A) mit der Buchse “DC +5V, 3A” des mGuards.
- Verbinden Sie den lokalen Computer oder das lokale Netzwerk mittels eines UTP Ethernetkabels (CAT 5) mit einem der Ethernet LAN Anschlüsse (4 bis 7) des mGuards.

4.6 mGuard PCI installieren

Warnung:

! Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

4.6.1 Auswahl Treibermodus oder Power-over-PCI Modus

Es gibt zwei Betriebsmodi: *Treibermodus* und *Power-over-PCI Modus.*

Der mGuard wird per Jumper auf den gewünschten Modus geschaltet.

Treibermodus:

Der mGuard PCI kann wie eine normale Netzwerkkarte verwendet werden. Dann stellt diese Netzwerkkarte zusätzlich die mGuard Funktionen zur Verfügung. In diesem Fall muss der mitgelieferte Treiber installiert werden.

Power-over-PCI Modus:

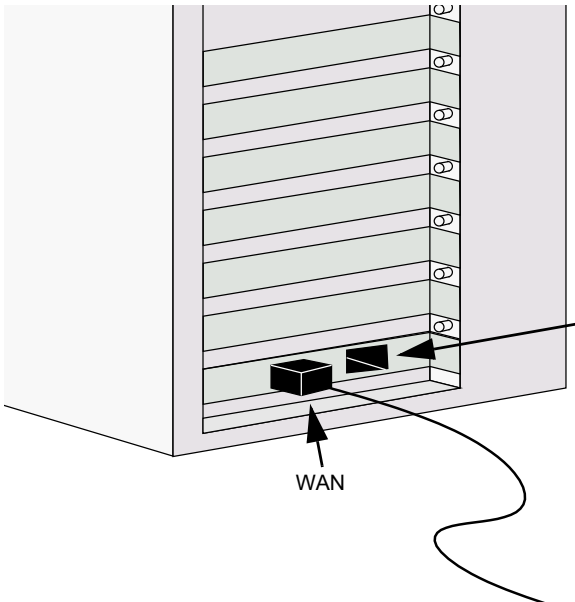
Wenn die Netzwerkkarten-Funktionalität des mGuard nicht gebraucht wird oder nicht verwendet werden soll, kann der mGuard PCI hinter eine vorhandene Netzwerkkarte (desselben Rechners oder eines anderen) quasi wie ein mGuard Standalone-Gerät angeschlossen werden. Tatsächlich steckt der mGuard PCI in dieser Betriebsart nur deswegen im PCI-Slot eines Rechners, um mit Strom versorgt zu werden und ein Gehäuse zu haben. Diese Betriebsart des mGuard wird *Power-over-PCI Modus* genannt. Ein Treiber wird nicht installiert.

Entscheiden Sie vor dem Einbau in Ihren PC, in welchem Modus Sie den mGuard PCI betreiben möchten.

Treibermodus

In diesem Modus muss später ein Treiber für die PCI Schnittstelle des mGuard PCI (verfügbar für Windows XP/2000 und Linux) auf dem Computer installiert werden. Im Treibermodus wird keine weitere Netzwerkkarte für den Computer benötigt.

Stealth-Modus im Treibermodus (Werkseinstellung)



Im Treibermodus ist die LAN Ethernet Buchse ausgeschaltet.

Die LAN-Schnittstelle des mGuard ist intern durch den Wirtsrechner belegt.

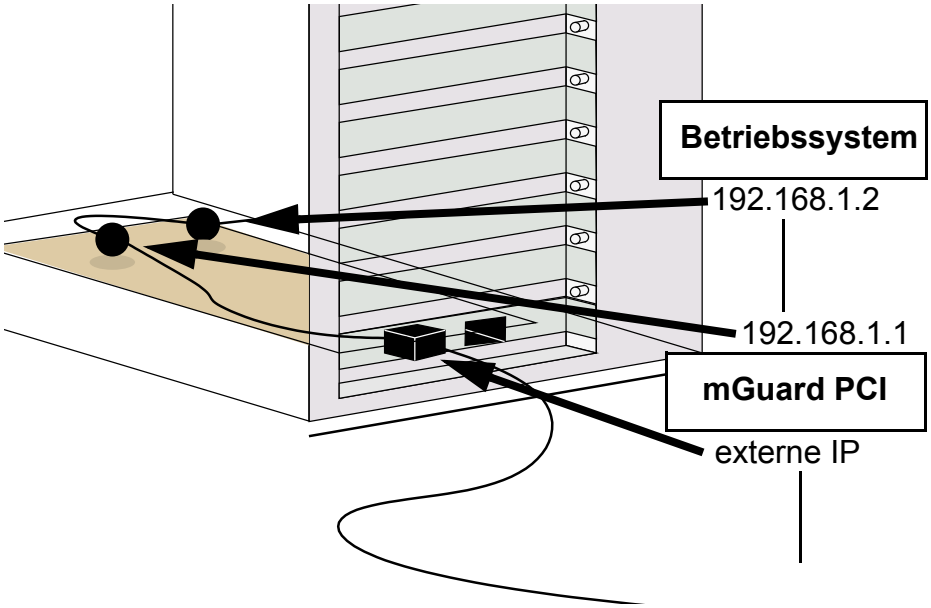
Im *Stealth*-Modus verhält sich der mGuard wie eine normale Netzwerkkarte.

Die IP-Adresse, die für die Netzwerkschnittstelle des Betriebssystems konfiguriert wird (= LAN Port), übernimmt der mGuard auch für seinen WAN-Port. Somit tritt der mGuard für den Datenverkehr vom und zum Rechner als

eigenes Gerät mit eigener Adresse gar nicht in Erscheinung.

⌦ Im Stealth-Modus ist es nicht möglich PPPoE oder PPTP zu verwenden.

Router Modus im Treibermodus



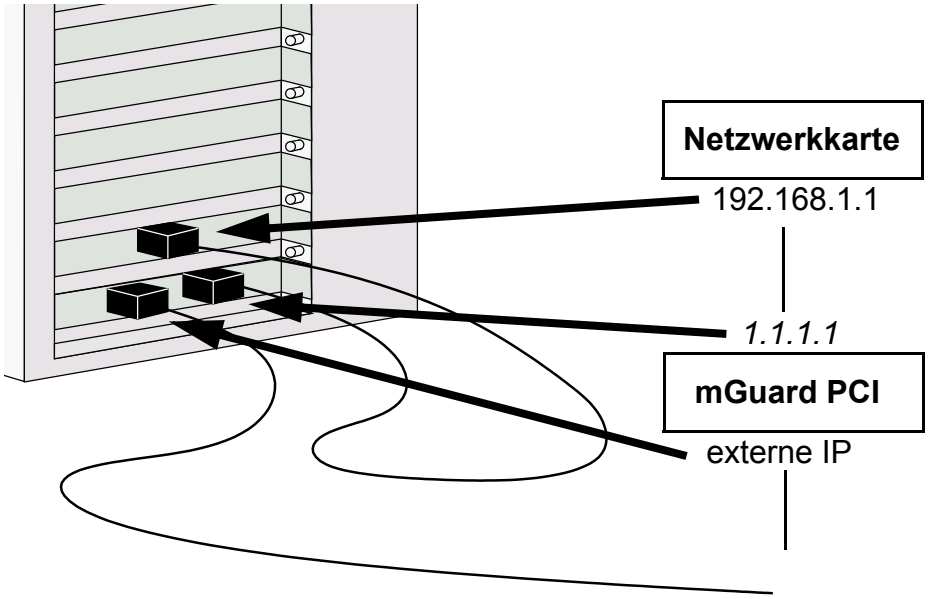
Befindet sich der mGuard im *Router*-Modus (oder *PPPoE*- oder *PPTP*-Modus), bildet er mit dem Betriebssystem des Rechners, in dem der mGuard installiert ist, quasi ein eigenes Netzwerk. Für die IP-Konfiguration der Netzwerkschnittstelle des Betriebssystems bedeutet das Folgendes: Dieser muss eine IP-Adresse zugewiesen werden, die sich von der internen IP-Adresse des mGuard (gemäß werkseitiger Voreinstellung 192.168.1.1) unterscheidet.

(Dieser Zusammenhang wird in der obiger Zeichnung durch zwei schwarze Kugeln verdeutlicht.)

Eine dritte IP-Adresse wird für die Schnittstelle des mGuard zum WAN verwendet. Über diese geht die Verbindung zu einem externen Netz (z. B. Internet).

Power-over-PCI Modus

Stealth-Modus im Power-over-PCI Modus

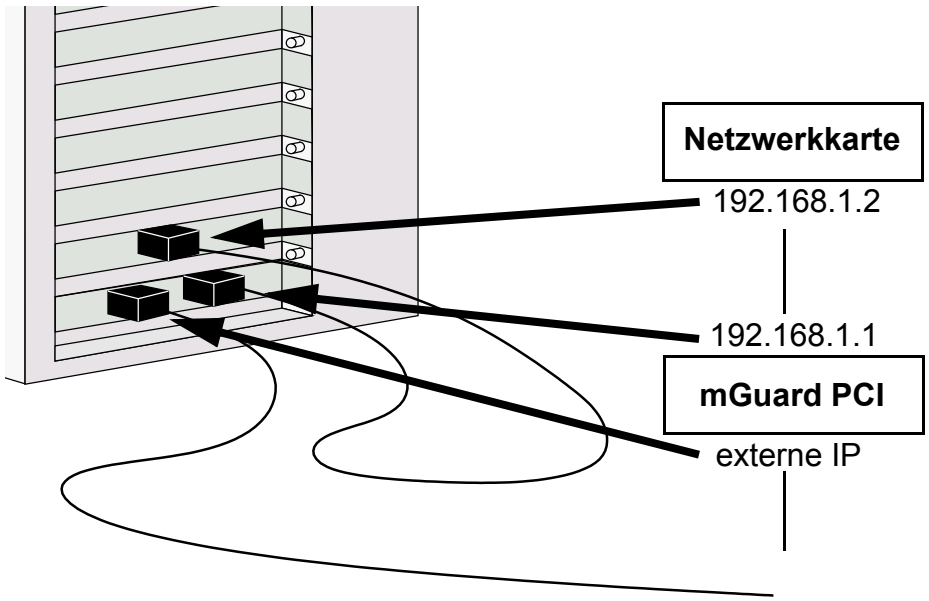


Da im Power-over-PCI Modus die Netzwerkkarten-Funktionalität des mGuard PCI ausgeschaltet ist, wird für ihn keine Treibersoftware installiert. An den LAN Port des mGuard PCI wird eine bereits installierte Netzwerkkarte angeschlossen, die sich im gleichen oder in einem anderen Computer befindet. (Siehe “Einbau der Hardware” auf Seite 40.)

Im *Stealth*-Modus wird die IP-Adresse, die für die Netzwerkschnittstelle des Betriebssystems (= LAN Port) konfiguriert ist, vom mGuard auch für seinen WAN Port übernommen. Somit tritt der mGuard für den Datenverkehr vom und zum Rechner als eigenes Gerät mit eigener Adresse gar nicht in Erscheinung.

⌦ Im Stealth-Modus ist es nicht möglich PPPoE oder PPTP zu verwenden.

Router Modus im Power-over-PCI-Modus

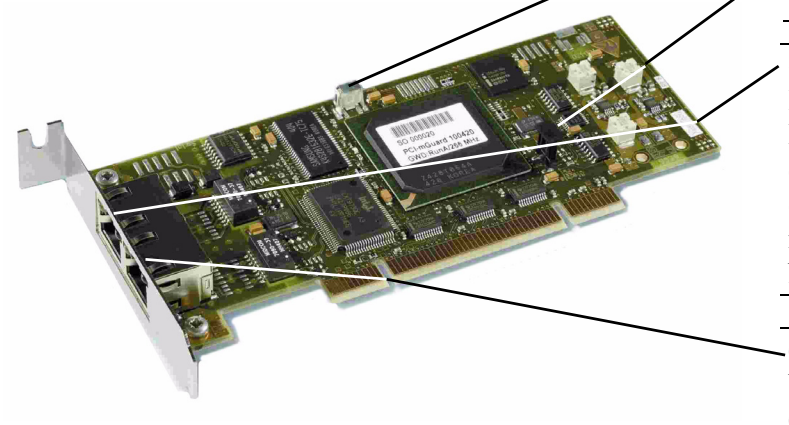


Befindet sich der mGuard im *Router*-Modus (oder *PPPoE* oder *PPTP* Modus), arbeiten der mGuard und die an seiner LAN-Buchse angeschlossene Netzwerkkarte - installiert im selben Rechner oder einem anderen - wie ein eigenes Netzwerk.

Für die IP-Konfiguration der Netzwerkschnittstelle des Betriebssystem des Rechners, in dem die Netzwerkkarte installiert ist, bedeutet das Folgendes: Dieser Netzwerkschnittstelle muss eine IP-Adresse zugewiesen werden, die sich von der internen IP-Adresse des mGuard (gemäß werkseitiger Voreinstellung 192.168.1.1) unterscheidet.

Eine dritte IP-Adresse wird für die Schnittstelle des mGuard zum WAN verwendet. Über diese geht die Verbindung zu einem externen Netz (z. B. Internet).

4.6.2 Einbau der Hardware



(1) Rescue Knopf

(2) Jumper zum Aktivieren/Deaktivieren des Treibermodus

(3) LAN Port
Ist im Treibermodus deaktiviert. Im Power-over-PCI-Modus wird hier die Netzwerkkarte desselben oder eines anderen zu schützenden Rechners oder das zu schützende Netzwerk angeschlossen.

(4) WAN Port
Verbindungen zum externen Netz (z. B. Internet) werden über diese Schnittstelle aufgebaut. Gemäß Firewall-Werkseinstellung sind hier eingehende Verbindungen gesperrt. Verwenden Sie ein UTP Kabel

Warnung:

Vor dem Einbau den freien Metallrahmen des PCs berühren, in den Sie den mGuard PCI einbauen wollen, um Ihren Körper elektrostatisch zu entladen.

1. Konfigurieren Sie den mGuard für den *Treibermodus* oder *Power-over-PCI Modus*. (Siehe “Auswahl Treibermodus oder Power-over-PCI Modus” auf Seite 37.)
   Setzen Sie dazu den Jumper (2) an die entsprechende Position:

Treibermodus	**Power-over-PCI Modus**
3 2 1	3 2 1

2. Schalten Sie den Computer sowie andere angeschlossene Peripheriegeräte aus. Folgen Sie den Sicherheitshinweisen zur elektrostatischen Entladung.
3. Ziehen Sie das Stromkabel.
4. Öffnen Sie die Abdeckung des Computers. Bitte folgenden Sie dabei der Beschreibung im Handbuch des Computers.
5. Wählen Sie einen freien PCI Steckplatz (3.3V oder 5V) für den mGuard PCI.
6. Entfernen Sie das dazugehörige Slotblech durch Lösen der entsprechenden

Schraube und Herausziehen des Slotblechs. Bewahren Sie die Schraube für das Festschrauben der mGuard PCI Karte auf.

7. Richten Sie die Steckerleiste der mGuard PCI Karte vorsichtig über der Buchsenleiste des PCI Steckplatzes auf dem Motherboard aus, und drücken Sie anschließend die Karte gleichmäßig in die Buchsenleiste hinein.
8. Schrauben Sie das Slotblech der Karte fest.
9. Schließen Sie die Abdeckung des Computers wieder.
10. Schließen Sie das Stromkabel des Computers wieder an und schalten Sie diesen ein.

4.6.3 Treiberinstallation

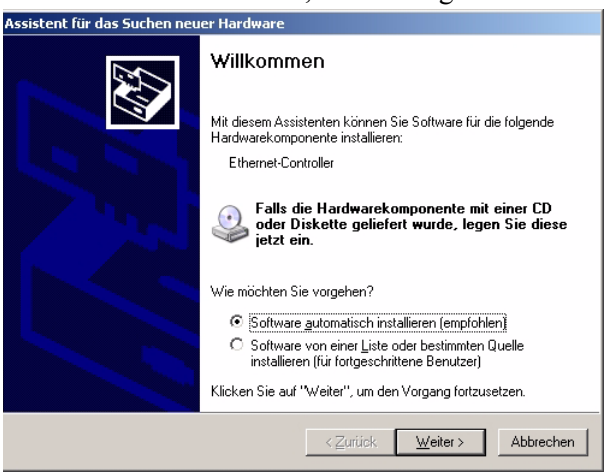
⌦ Nur wenn der mGuard PCI im *Treibermodus* arbeitet, ist die Installation eines Treibers erforderlich und möglich (siehe „Treibermodus" auf Seite 37).

Voraussetzungen

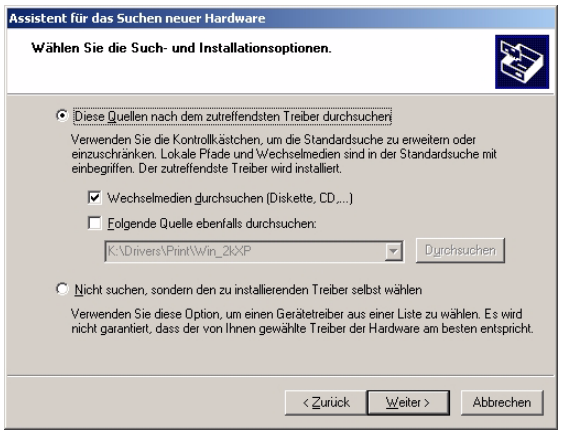
- Falls noch nicht geschehen, führen Sie die unter „Einbau der Hardware" auf Seite 40 beschriebenen Schritte aus.
- Sie haben die Treiberdateien auf einem Datenträger.
  Falls nicht: Erhältlich sind die Treiberdateien im Download-Bereich der Website www.innominate.com, herunterladbar als ZIP-Archiv. Entpacken Sie das ZIP-Archiv. Brennen bzw. kopieren Sie die entpackten Dateien auf einen Datenträger - z. B. CD, USB-Speicherstick oder Diskette.

Unter Windows XP

Nach Einbau der Hardware den Computer einschalten. Melden sich mit Administratorrechten an und warten Sie, bis das folgende Fenster erscheint:


Assistent für das Suchen neuer Hardware
Willkommen
Mit diesem Assistenten können Sie Software für die folgende Hardwarekomponente installieren:
Ethernet-Controller
Falls die Hardwarekomponente mit einer CD oder Diskette geliefert wurde, legen Sie diese jetzt ein.
Wie möchten Sie vorgehen?
Software automatisch installieren (empfohlen)
Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer)
Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.
< Zurück
Weiter >
Abbrechen

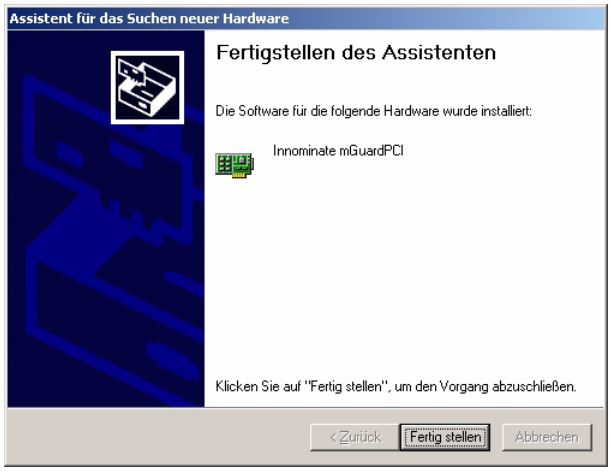
1. Nach Einlegen bzw. Einstecken des Datenträgers wählen Sie **Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer**) und klicken Sie auf **Weiter**.


Assistent für das Suchen neuer Hardware
Wählen Sie die Such- und Installationsoptionen.
Diese Quellen nach dem zutreffendsten Treiber durchsuchen
Verwenden Sie die Kontrollkästchen, um die Standardsuche zu erweitern oder einzuschränken. Lokale Pfade und Wechselmedien sind in der Standardsuche mit einbegriffen. Der zutreffendste Treiber wird installiert.
Wechselmedien durchsuchen (Diskette, CD,...)
Folgende Quelle ebenfalls durchsuchen:
K:\Drivers\Print\Win_2k\XP
Durchsuchen
Nicht suchen, sondern den zu installierenden Treiber selbst wählen
Verwenden Sie diese Option, um einen Gerätetreiber aus einer Liste zu wählen. Es wird nicht garantiert, dass der von Ihnen gewählte Treiber der Hardware am besten entspricht.
< Zurück
Weiter >
Abbrechen

2. Klicken Sie auf **Weiter**.

Hardwareinstallation
Die Software, die für diese Hardware installiert wird:
Innominate mGuardPCI
hat den Windows-Logo-Test nicht bestanden, der die Kompatibilität mit Windows XP überprüft. (Warum ist dieser Test wichtig?)
Das Fortsetzen der Installation dieser Software kann die korrekte Funktion des Systems direkt oder in Zukunft beeinträchtigen. Microsoft empfiehlt strengstens, die Installation jetzt abzubrechen und sich mit dem Hardwarehersteller für Software, die den Windows-Logo-Test bestanden hat, in Verbindung zu setzen.
Installation fortsetzen
Installation abbrechen

3. Klicken Sie auf **Installation fortsetzen**.


Assistent für das Suchen neuer Hardware
Fertigstellen des Assistenten
Die Software für die folgende Hardware wurde installiert:
Innominate mGuardPCI
Klicken Sie auf "Fertig stellen", um den Vorgang abzuschließen.
< Zurück
Fertig stellen
Abbrechen

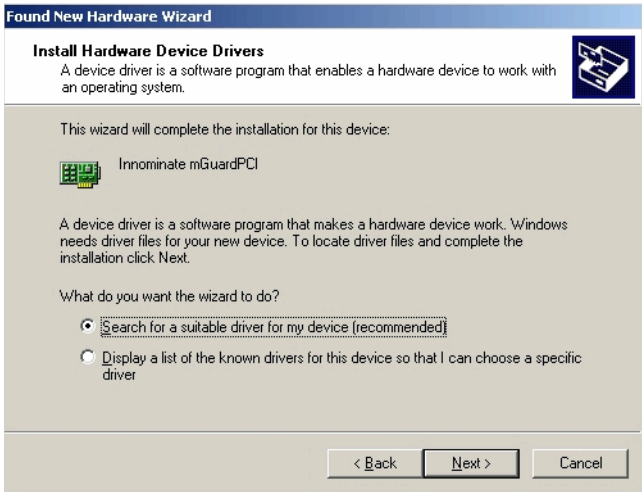
4. Klicken Sie auf **Fertig stellen**.

Unter Windows 2000

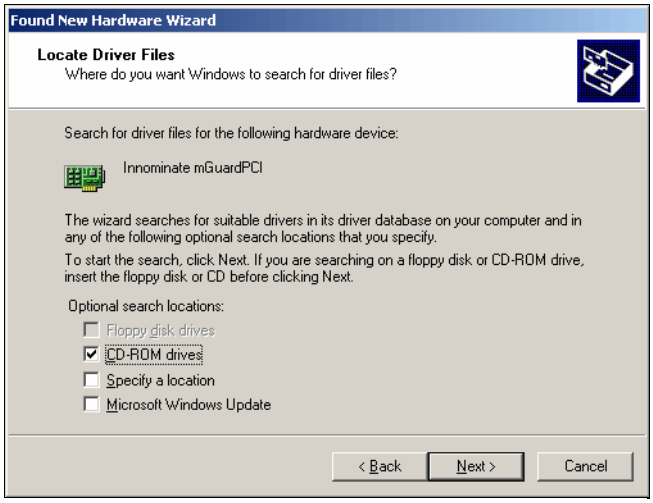
Nach Einbau der Hardware den Computer einschalten. Melden sich mit Administratorrechten an und warten Sie, bis das folgende Fenster erscheint:

Found New Hardware Wizard
Welcome to the Found New Hardware Wizard
This wizard helps you install a device driver for a hardware device.
To continue, click Next.
< Back
Next >
Cancel

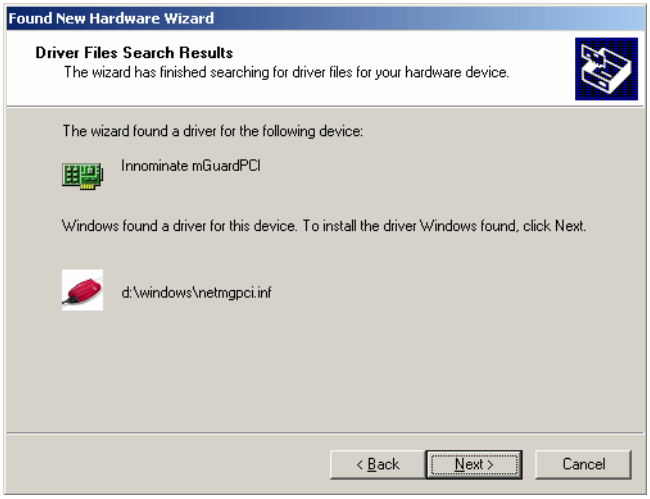
1. Klicken Sie auf **Weiter**.


Found New Hardware Wizard
Install Hardware Device Drivers
A device driver is a software program that enables a hardware device to work with an operating system.
This wizard will complete the installation for this device:
Innominate mGuardPCI
A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.
What do you want the wizard to do?
Search for a suitable driver for my device (recommended)
Display a list of the known drivers for this device so that I can choose a specific driver
< Back
Next >
Cancel

2. Wählen Sie **Suche nach einem passenden Treiber für das Gerät** und klicken Sie auf **Weiter**.


Found New Hardware Wizard
Locate Driver Files
Where do you want Windows to search for driver files?
Search for driver files for the following hardware device:
Innominate mGuardPCI
The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.
To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.
Optional search locations:
Floppy disk drives
CD-ROM drives
Specify a location
Microsoft Windows Update
< Back
Next >
Cancel

3. Wählen Sie **Specify a location** und klicken Sie auf **Weiter**.


Found New Hardware Wizard
Driver Files Search Results
The wizard has finished searching for driver files for your hardware device.
The wizard found a driver for the following device:
Innominate mGuardPCI
Windows found a driver for this device. To install the driver Windows found, click Next.
d:\windows\netmgpci.inf
< Back
Next >
Cancel

4. Klicken Sie auf **Weiter**.

Digital Signature Not Found
The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.
Innominate mGuardPCI
If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.
Do you want to continue the installation?
Yes
No
More Info

5. Klicken Sie auf **Ja**.

6. Klicken Sie auf **Fertigstellen**.

Unter Linux

Der Linuxtreiber ist im Sourcecode verfügbar und muss vor Verwendung übersetzt werden:

- Bauen und übersetzen Sie zunächst den Linuxkernel (2.4.25) im Verzeichnis **/usr/src/linux**
- Entpacken Sie die Treiber des ZIP-Archivs ins Verzeichnis **/usr/src/pci-driver**
- Führen Sie die folgenden Kommandos aus
    - **cd /usr/src/pci-driver**
    - **make LINUXDIR=/usr/src/linux**
    - **install -m0644 mguard.o /lib/modules/2.4.25/kernel/drivers/net/**
    - **depmod -a**
- Der Treiber kann nun mit dem folgenden Kommando geladen werden
    - **modprobe mguard**

5 Konfiguration vorbereiten

5.1 Anschlussvoraussetzungen

mGuard industrial RS

- Der mGuard industrial RS muss an mindestens einem aktivem Netzteil angeschlossen sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des mGuard angeschlossen sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

mGuard smart

- Der mGuard smart muss eingeschaltet sein, d. h. per USB-Kabel an einen eingeschalteten Rechner (oder Netzteil) angeschlossen sein, so dass er mit Strom versorgt wird.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – am LAN Port des mGuard angeschlossen sein,
  – oder er muss über das lokale Netzwerk mit dem mGuard verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

mGuard PCI

- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss folgende Voraussetzungen erfüllen:
  mGuard im *Treibermodus*: Auf dem Rechner muss der mGuard PCI Treiber installiert sein.
  mGuard im *Power-over-PCI Modus*: Der Rechner muss am LAN-Anschluss des mGuard angeschlossen sein oder über das lokale Netzwerk mit dem mGuard verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

mGuard blade

- Der mGuard blade muss in der mGuard bladeBase montiert sein, und mindestens eines der Netzteile der bladeBase muss in Betrieb sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – an der LAN-Buchse des mGuard angeschlossen sein,
  – oder der Rechner muss über das Netzwerk mit dem mGuard verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

EAGLE mGuard

- Der EAGLE mGuard muss an mindestens einem aktivem Netzteil angeschlossen sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – an der LAN-Buchse des mGuard angeschlossen sein,
  – oder der Rechner muss über das Netzwerk mit dem mGuard verbunden sein.

- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

mGuard delta

- Der mGuard delta muss an seine Stromversorgung angeschlossen sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – am LAN Switch (Ethernetbuchse 4 bis 7) des mGuard angeschlossen sein,
  – oder er muss über das lokale Netzwerk mit dem mGuard verbunden sein.
- Bei Fernkonfiguration: Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

5.2 Lokale Konfiguration: Bei Inbetriebnahme

Der mGuard wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird (z. B. MS Internet-Explorer ab Version 5.0, Mozilla Firefox ab Version 1.5 oder Safari).

⌧ Der Web-Browser muss SSL (d. h. https) unterstützen.

Der mGuard ist gemäß Werkseinstellung unter folgender Adressen erreichbar:

Werkseinstellung:

Stealth-Modus: (Auslieferungszustand, bis auf mGuard delta und blade Kontroller)	https://1.1.1.1/
Router-Modus: (Auslieferungszustand mGuard delta und blade Kontroller)	https://192.168.1.1/

5.2.1 mGuard industrial RS, mGuard smart, mGuard blade und EAGLE mGuard

Bei konfigurierter Netzwerkschnittstelle

Damit der mGuard über die Adresse https://1.1.1.1/ angesprochen werden kann, muss er an eine konfigurierte Netzwerkschnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt - siehe Abbildung im Abschnitt

- „mGuard smart anschließen“ auf Seite 30.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des mGuard herstellen - siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 53. Fahren Sie in diesem Falle dort fort.

Bei nicht konfigurierter Netzwerkschnittstelle

Falls die Netzwerkschnittstelle des Rechners nicht konfiguriert ist...

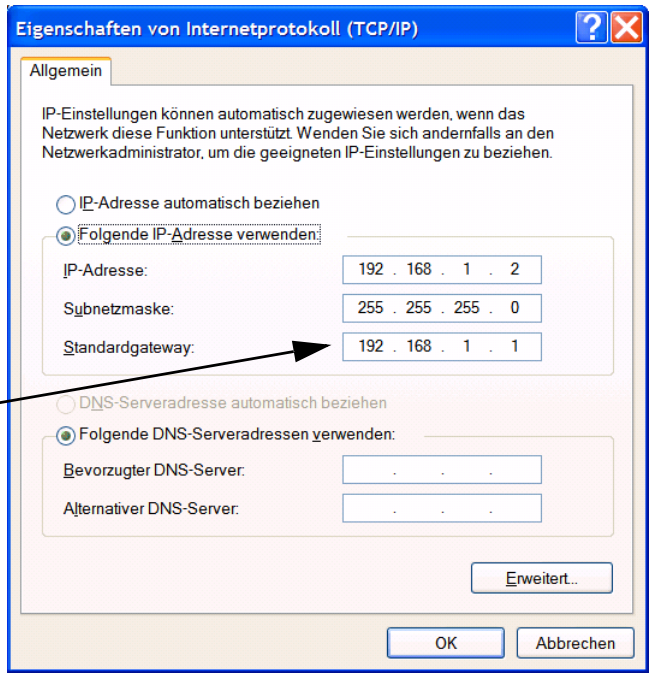
Wenn der Konfigurations-Rechner noch nicht an einem Netzwerk angeschlossen war, z. B. weil der Rechner neu ist, dann ist seine Netzwerkschnittstelle im Allgemeinen nicht konfiguriert. Das heißt der Rechner „weiß“ noch nicht, dass der Netzwerkverkehr über diese Schnittstelle läuft.

In diesem Fall müssen Sie das Standardgateway initialisieren, indem Sie ihm einen Dummy-Wert zuweisen. Gehen Sie dazu wie folgt vor:

Standardgateway initialisieren

1. Ermitteln Sie die zurzeit gültige Standardgateway-Adresse. Unter Windows XP gehen Sie dazu wie folgt vor:
   – **Start, Systemsteuerung, Netzwerkverbindungen** klicken.
   – Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet. Im Kontextmenü **Eigenschaften** klicken.
   – Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren. Dann die

Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfenster angezeigt wird:


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Hier die IP-Adresse des Standardgateway nachschlagen oder festlegen.

Falls in diesem Dialogfeld keine IP-Adresse des Standardgateway angegeben ist, z. B. weil *IP-Adresse automatisch beziehen* aktiviert ist, dann geben Sie eine IP-Adresse manuell ein. Dazu aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.1

⌦ Auf keinen Fall dem Konfigurations-Rechner eine Adresse wie 1.1.1.2 geben!

2. Auf DOS-Ebene (Menü **Start, Alle Programme, Zubehör, Eingabeaufforderung**) geben Sie ein:
   `arp -s` <IP des Standardgateway> **`00-aa-aa-aa-aa-aa`**
   Beispiel:
   Sie haben als Standardgateway-Adresse ermittelt oder festgelegt: 192.168.1.1
   Dann lautet der Befehl:
   `arp -s 192.168.1.1 00-aa-aa-aa-aa-aa`

3. Zur Konfiguration stellen Sie jetzt die Konfigurationsverbindung her - siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 53

4. Nach der Konfiguration stellen Sie das Standardgateway wieder zurück. Dazu entweder den Konfigurations-Rechner neu starten oder auf DOS-Ebene folgendes Kommando eingeben:
   `arp -d`

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.2.2 mGuard delta

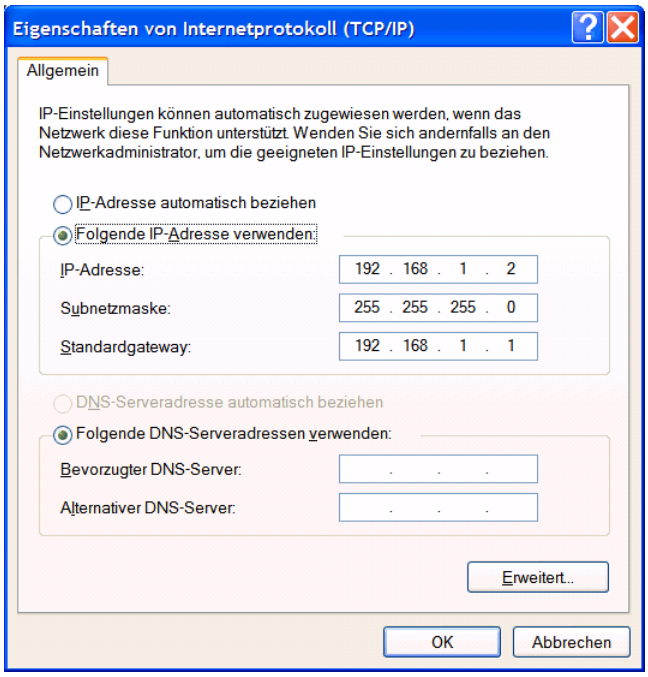
Bei Auslieferung oder nach Zurücksetzen auf die Werkseinstellung oder Flashen des mGuards ist der mGuard delta über die LAN Schnittstellen 4 bis 7 unter der IP Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar. Für einen Zugriff auf die Konfigurationsoberfläche kann es daher nötig sein, die Konfiguration Ihres Computers anzupassen.

Unter Windows XP gehen Sie dazu wie folgt vor:

– **Start, Systemsteuerung, Netzwerkverbindungen** klicken.

– Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet. Im Kontextmenü **Eigenschaften** klicken.

– Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren. Dann die Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfenster angezeigt wird:


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.1

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.2.3 mGuard PCI

Installieren der PCI Karte

Wenn Sie die PCI Karte noch nicht in ihrem Computer installiert haben, folgen Sie bitte zunächst den unter „Einbau der Hardware“ auf Seite 40 beschriebenen Schritten.

Installieren der Treiber

Wenn Sie den mGuard für den **Treibermodus** konfiguriert haben, stellen Sie bitte sicher, dass die Treiber wie unter „Treiberinstallation“ auf Seite 41 beschrieben installiert sind.

Konfiguration der Netzwerkschnittstelle

Wenn Sie den mGuard

- im **Treibermodus** betreiben und die LAN-Schnittstelle (= Netzwerkschnittstelle des Computers) noch nicht konfiguriert wurde
  ODER
- im **Power-over-PCI Modus** betreiben und die Netzwerkschnittstelle des Computers, der am LAN Interface des mGuards angeschlossenen ist, noch nicht konfiguriert wurde

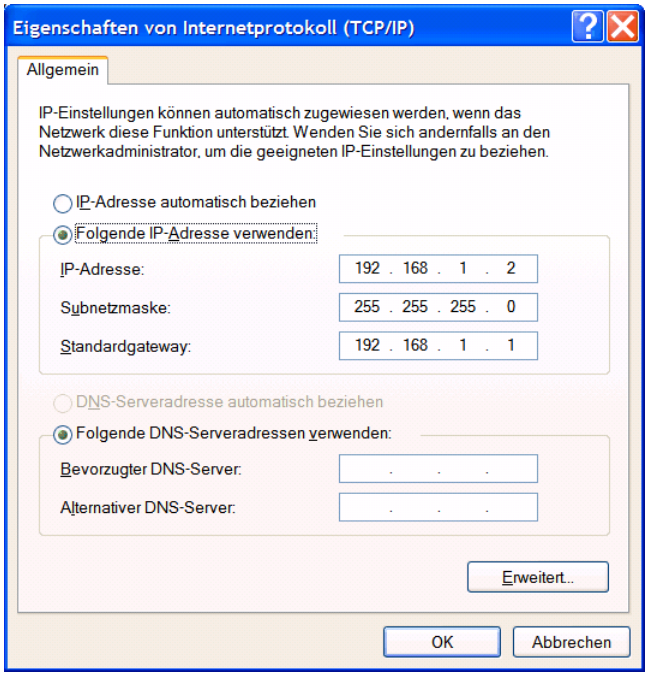
dann müssen Sie diese Netzwerkschnittstelle konfigurieren, bevor Sie den mGuard konfigurieren können.

Unter Windows XP konfigurieren Sie die Netzwerkschnittstelle wie folgt:

– **Start, Systemsteuerung, Netzwerkverbindungen** klicken.

– Das Symbol des LAN-Adapters mit der rechten Maustaste klicken, so dass sich das Kontextmenü öffnet. Im Kontextmenü **Eigenschaften** klicken.

– Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren. Dann die Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfenster angezeigt wird:


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Standardgateway

Nachdem Sie die Netzwerkschnittstelle konfiguriert haben, sollten Sie die Konfigurationsoberfläche des mGuards mit einem Webbrowser unter der URL „https://1.1.1.1/“ erreichen können. Wenn dies nicht möglich ist, dann ist möglicherweise das Standardgateway ihres Computers nicht erreichbar. In diesem Fall muss es ihrem Computer wie folgt vorgetäuscht werden:

Standardgateway initialisieren

1. Ermitteln Sie die zurzeit gültige Standardgateway-Adresse.

Unter Windows XP folgen Sie dazu den oben (unter „Konfiguration der Netzwerkschnittstelle“ auf Seite 51) beschriebenen Schritten, um das Dialogfeld **Eigenschaften von Internetprotokoll (TCP/IP)** zu öffnen.
Falls in diesem Dialogfeld keine IP-Adresse des Standardgateway angegeben ist, z. B. weil *IP-Adresse automatisch beziehen* aktiviert ist, dann geben Sie eine IP-Adressen manuell ein. Dazu aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.1

⌦ Auf keinen Fall dem Konfigurations-Rechner eine Adresse wie 1.1.1.2 geben!

2. Auf DOS-Ebene (Menü **Start, Alle Programme, Zubehör, Eingabeaufforderung**) geben Sie ein:
   `arp -s` <IP des Standardgateway> **`00-aa-aa-aa-aa-aa`**
   Beispiel:
   Sie haben als Standardgateway-Adresse ermittelt oder festgelegt: 192.168.1.1
   Dann lautet der Befehl:
   `arp -s 192.168.1.1 00-aa-aa-aa-aa-aa`

3. Zur Konfiguration stellen Sie jetzt die Konfigurationsverbindung her - siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 53

4. Nach der Konfiguration stellen Sie das Standardgateway wieder zurück. Dazu entweder den Konfigurations-Rechner neu starten oder auf DOS-Ebene folgendes Kommando eingeben:
   `arp -d`

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.3 Lokale Konfigurationsverbindung herstellen

Web-basierte Administrator-oberfläche

Der mGuard wird per Web-Browser (z. B. Firefox, MS Internet-Explorer oder Safari) konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

⌧ Der Web-Browser muss SSL (d. h. https) unterstützen.

Der mGuard wird je nach Modell entweder im Netzwerk-Modus ***Stealth*** oder ***Router*** ausgeliefert und ist dem entsprechend unter einer der folgenden Adressen erreichbar:

Werkseinstellung:

Stealth-Modus: (Auslieferungszustand, bis auf mGuard delta und blade Kontroller)	https://1.1.1.1/
Router-Modus: (Auslieferungszustand mGuard delta und blade Kontroller)	https://192.168.1.1/

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser.
   (Z. B. Firefox, MS Internet-Explorer oder Safari; der Web-Browser muss SSL (d. h. https) unterstützen.)
2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum mGuard erschwert werden könnte.
   Im MS Internet Explorer nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*:
   Unter *DFÜ- und VPN-Einstellungen* muss **Keine Verbindung wählen** aktiviert sein.
3. In der Adresszeile des Web-Browsers geben Sie die Adresse des mGuard vollständig ein.
   Im **Stealth**-Modus (= Werkseinstellung außer mGuard delta und blade Kontroller) lautet diese immer

   `https://1.1.1.1/`

   und in den Betriebsarten **Router** (= Werkseinstellung mGuard delta und blade Kontroller), **PPPoE** oder **PPTP** lautet diese immer

   `https://192.168.1.1/`

   Folge:
   Sie gelangen zur Administrator-Webseite des mGuard. Der auf der nächsten Seite abgebildete Sicherheitshinweis erscheint.

IP-Adresse des mGuard im *Stealth*-Modus: **https://1.1.1.1/**

wenn nicht im *Stealth*-Modus: **https://192.168.1.1/**

⌧ Falls Sie die konfigurierte Adresse vergessen haben:

Falls die Adresse des mGuard im *Router- PPPoE-* oder *PPTP*-Modus auf einen anderen Wert gesetzt ist, und Sie kennen die aktuelle Adresse nicht, dann müssen Sie den mGuard mit Hilfe der **Recovery**-Taste in den Stealth-Modus (mGuard delta und blade Kontroller: Router-Modus) stellen, sodass die oben angegebenen Werkseinstellungen bezüglich der IP-Adresse des mGuard wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 265).

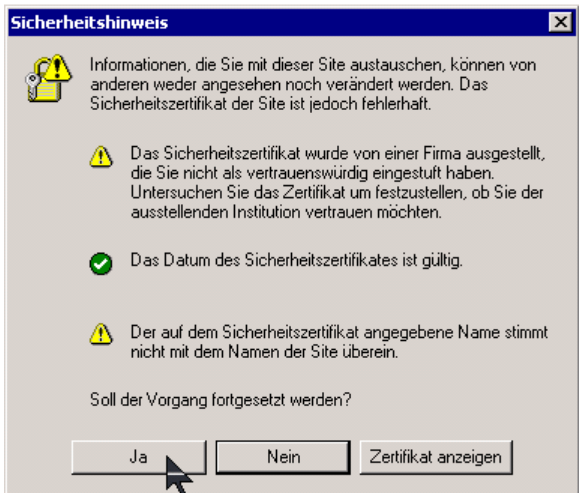
⌦ Falls die Administrator-Webseite nicht angezeigt wird...

Sollte auch nach wiederholtem Versuch der Web-Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Prüfen Sie, ob der Standardgateway des angeschlossenen Konfigurations-Rechners initialisiert ist. Siehe „Lokale Konfiguration: Bei Inbetriebnahme“ auf Seite 48
- Bestehende Firewalls gegebenenfalls deaktivieren.
- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet.
  Im MS Internet Explorer (Version 6.0) nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*: Unter *LAN-Einstellungen* auf die Schaltfläche **Einstellungen...** klicken, im Dialogfeld *Einstellungen für lokales Netzwerk (LAN)* dafür sorgen, dass unter Proxyserver der Eintrag **Proxyserver für LAN verwenden** nicht aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü **Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen** bzw. **Netzwerk- und DFÜ-Verbindungen** das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü **Deaktivieren** wählen.

Bei erfolgreichem Verbindungsaufbau

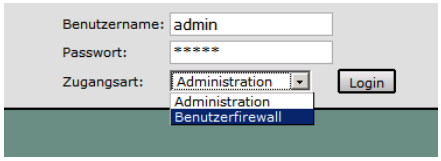
Nach erfolgreicher Verbindungsaufnahme erscheint dieser Sicherheitshinweis (MS Internet-Explorer):


Sicherheitshinweis
Informationen, die Sie mit dieser Site austauschen, können von anderen weder angesehen noch verändert werden. Das Sicherheitszertifikat der Site ist jedoch fehlerhaft.
Das Sicherheitszertifikat wurde von einer Firma ausgestellt, die Sie nicht als vertrauenswürdig eingestuft haben. Untersuchen Sie das Zertifikat um festzustellen, ob Sie der ausstellenden Institution vertrauen möchten.
Das Datum des Sicherheitszertifikates ist gültig.
Der auf dem Sicherheitszertifikat angegebene Name stimmt nicht mit dem Namen der Site überein.
Soll der Vorgang fortgesetzt werden?
Ja
Nein
Zertifikat anzeigen

Erläuterung:
Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

Quittieren Sie den entsprechenden Sicherheitshinweis mit **Ja**.

Folge:
Das Login-Fenster wird angezeigt.



Wählen Sie die Zugangsart — Administration oder Benutzerfirewall — und geben Sie Ihren Benutzernamen und Ihr Passwort ein, die für diese Zugangsart festgelegt ist. (Benutzerfirewall siehe „Netzwerksicherheit » Benutzerfirewall“ auf Seite 190)

Für Administration ist werkseitig voreingestellt:

Benutzername: `admin`
Passwort: `mGuard`

⌦ Groß- und Kleinschreibung beachten!

Zur Konfiguration machen Sie auf den einzelnen Seiten der Oberfläche des mGuard die gewünschten bzw. erforderlichen Angaben.
Siehe „Konfiguration“ auf Seite 57.

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern - siehe „Authentifizierung » Lokale Benutzer“ auf Seite 158 .

5.4 Fernkonfiguration

Voraussetzung

Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

⌦ Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Um die Möglichkeit zur Fernkonfiguration einzuschalten, siehe Abschnitt „Verwaltung » Web Einstellungen“, „Zugriff“ auf Seite 75.

Fernkonfiguration

Um von einem entfernten Rechner aus den mGuard über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum mGuard her.
Gehen Sie wie folgt vor:

1. Starten Sie dazu auf dem entfernten Rechner den Web-Browser (z. B.Firefox, MS Internet-Explorer oder Safari; der Web-Browser muss HTTPS unterstützen).
2. Als Adresse geben Sie an: Die IP-Adresse, unter der der mGuard von extern über das Internet bzw. WAN erreichbar ist, gegebenenfalls zusätzlich die Port-Nummer.

   Beispiel:
   Ist dieser mGuard über die Adresse https://123.45.67.89/ über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/
   Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B.: https://123.45.67.89:442/

Zur Konfiguration machen Sie auf den einzelnen Seiten der mGuard-Oberfläche die gewünschten bzw. erforderlichen Angaben.
Siehe „Konfiguration“ auf Seite 57.

6 Konfiguration

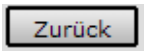
6.1 Bedienung

Bildschirmaufteilung

1. Über das Menü links den Eintrag für die Seite mit den gewünschten Einstellmöglichkeiten anklicken, z. B. *Verwaltung » Lizenzierung*. Dann wird im Hauptfenster die Seite angezeigt - in Form einer oder mehrerer Registerkarten - auf denen Sie Einstellungen vornehmen können. Gliedert sich eine Seite in mehrere Registerkarten, oben auf die Registerkartenzunge (auch *Tab* genannt) klicken, um zu blättern.
2. Auf der betreffenden Seite bzw. Registerkarte die gewünschten Einträge machen. Siehe dazu auch den nachfolgenden Unterabschnitt „Arbeiten mit sortierbaren Tabellen“ auf Seite 57.
3. Damit die Einstellungen vom Gerät übernommen werden, die Schaltfläche **Übernehmen** klicken.

Nach der Übernahme vom System erhalten Sie eine (bestätigende) Rückmeldung. Damit sind die neuen Einstellungen in Kraft. Sie bleiben in Kraft auch nach einem Neustart (Reset).

- Befindet sich unten rechts die Schaltfläche **Zurück**, kehren Sie durch Klicken auf diese Schaltfläche auf die Seite zurück, von der Sie gekommen sind.



Bei Eingabe unzulässiger Werte

Nach Eingabe unzulässiger Werte (z. B. einer unzulässigen Zahl in einer IP-Adresse) und nach anschließendem Klicken auf **Übernehmen** wird die Schrift des betreffenden Registerkarten-Titels in Rot dargestellt. Das erleichtert Ihnen das Auffinden des Fehlers.

Arbeiten mit sortierbaren Tabellen

Viele Einstellungen werden als Datensätze gespeichert. Entsprechend werden Ihnen die einstellbaren Parameter und deren Werte in Form von Tabellenzeilen präsentiert. Sind mehrere Datensätze mit Einstellungen gesetzt (z. B. Firewall-Regeln), werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt bzw. abgearbeitet. Gegebenenfalls ist also auf die Reihenfolge der Einträge zu achten. Durch das Verschieben von Tabellenzeilen nach unten oder oben kann die Reihenfolge geändert werden.

Bei Tabellen können Sie

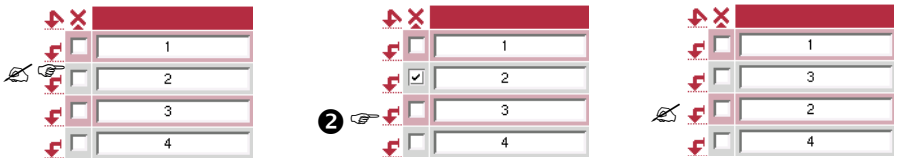
– Zeilen einfügen, um einen neuen Datensatz mit Einstellungen anzulegen (z. B. die Firewall-Einstellungen für eine bestimmte Verbindung)
– Zeilen verschieben (d. h. umsortieren) und
– Zeilen löschen, um den gesamten Datensatz zu löschen.

Einfügen von Zeilen

1. Klicken Sie auf den Pfeil, unter dem Sie eine neue Zeile einfügen wollen:

2. Folge: Die neue Zeile ist eingefügt.
Jetzt können Sie in der Zeile Werte eintragen oder angeben

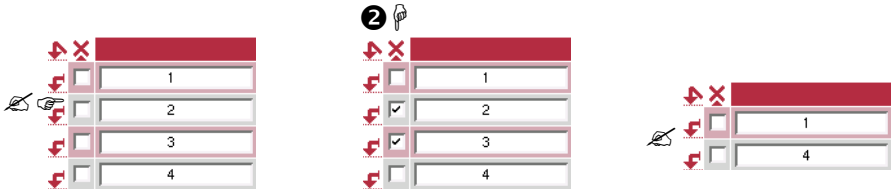
Verschieben von Zeilen



1. Markieren Sie eine oder mehrere Zeilen, die Sie verschieben wollen.
2. Klicken Sie auf den Pfeil, unter den Sie die markierten Zeilen verschieben wollen:

3. Folge: Die Zeilen sind verschoben.

Löschen von Zeilen



1. Markieren Sie die Zeilen, die Sie löschen wollen.
2. Klicken Sie auf das Zeichen zum Löschen:

3. Folge: Die Zeilen sind gelöscht.

Arbeiten mit nicht sortierbaren Tabellen

Tabellen, bei denen die Reihenfolge der in ihnen enthaltenen Datensätze technisch keine Rolle spielt, sind nicht sortierbar. Es ist also nicht möglich, Zeilen einzufügen oder zu verschieben. Bei solchen Tabellen können Sie

– Zeilen löschen - wie oben bei sortierbaren Tabellen - und
– Zeilen am Tabellenende anfügen, um einen neuen Datensatz mit Einstellungen anzulegen (z. B. Benutzerfirewall-Templates)

Entsprechend unterscheiden sich die Symbole zum Anfügen / Einfügen einer neuer Tabellenzeile:

für Anfügen bei nicht sortierbarer Tabelle

für Einfügen bei einer sortierbaren Tabelle

Anfügen von Zeilen (nicht sortierbare Tabelle)

1. Klicken Sie auf den Pfeil, um eine neue Zeile anzufügen:

2. Folge: Die neue Zeile wird unter der bestehenden Tabelle angefügt. Jetzt können Sie in der Zeile Werte eintragen oder angeben.

Weitere Bedienhinweise

Folgende Schaltflächen stehen auf dem Seitenkopf auf allen Seiten zur Verfügung:

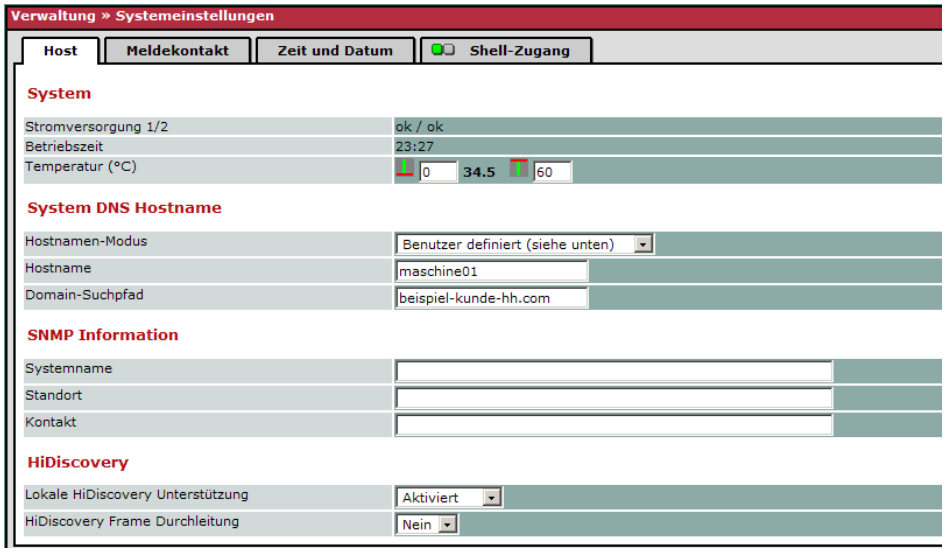
Logout	Zum Abmelden nach einem Konfigurations-Zugriff auf den mGuard. Führt der Benutzer kein Logout durch, wird ein Logout automatisch durchgeführt, sobald keine Aktivität mehr stattfindet und die durch die Konfiguration festgelegte Zeit abgelaufen ist. Ein erneuter Zugriff kann dann nur durch erneutes Anmelden (Login) erfolgen.
Reset	Optionale Schaltfläche. Zurücksetzen auf die alten Werte. Wenn Sie auf einer Konfigurationsseite Werte eingetragen haben und diese noch nicht mit **Übernehmen** in Kraft gesetzt haben, können Sie mit **Reset** die Seite auf die alten Werte zurücksetzen. Diese Schaltfläche ist nur dann im Kopfbereich der Seite eingeblendet, wenn der Gültigkeitsbereich der **Übernehmen**-Schaltfläche auf *seitenübergreifend* gestellt ist - siehe „Verwaltung » Web Einstellungen“ auf Seite 74.
Apply	Optionale Schaltfläche. Wirkt wie die Schaltfläche **Übernehmen**, gilt aber seitenübergreifend. Diese Schaltfläche ist nur dann im Kopfbereich der Seite eingeblendet, wenn der Gültigkeitsbereich der **Übernehmen**-Schaltfläche auf *seitenübergreifend* gestellt ist - siehe „Verwaltung » Web Einstellungen“ auf Seite 74.

6.2 Menü Verwaltung

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern - siehe „Authentifizierung » Lokale Benutzer“ auf Seite 158. Solange dies noch nicht geschehen ist, erhalten Sie oben auf der Seite einen Hinweis darauf.

6.2.1 *Verwaltung » Systemeinstellungen*

Host



System (nur mGuard industrial RS, EAGLE mGuard)

Power supply 1 / 2

Zustand der beiden Netzteile.

Betriebszeit

Bisherige Laufzeit des Geräts seit dem letzten Neustart.

Temperatur (°C)

Wenn der hier angegebene Temperaturbereich unter- bzw. überschritten wird, dann wird ein SNMP-Trap ausgelöst.

System DNS Hostname

Hostnamen Modus

Mit *Hostnamen Modus* und *Hostname* können Sie dem mGuard einen Namen geben. Dieser wird dann z. B. beim Einloggen per SSH angezeigt (siehe „Verwaltung » Systemeinstellungen“, „Shell-Zugang“ auf Seite 67). Eine Namensgebung erleichtert die Administration mehrerer mGuards.

Benutzerdefiniert (siehe unten)

(Standard) Der im Feld **Hostname** eingetragene Name wird als Name für den mGuard gesetzt.

☞ Arbeitet der mGuard im *Stealth*-Modus, muss als *Hostnamen Modus* die Option *Benutzer definiert* gewählt werden.

Provider definiert (z. B. via DHCP)

Sofern der Netzwerkmodus ein externes Setzen des Hostnamens erlaubt wie z. B. bei DHCP, dann wird der vom Provider übermittelte Name für den mGuard gesetzt.

Hostname

Ist unter *Hostnamen Modus* die Option *Benutzer definiert* ausgewählt, dann tragen Sie hier den Namen ein, den der mGuard erhalten soll.

Sonst, d. h. wenn unter *Hostnamen Modus* die Option *Provider definiert (z. B. via DHCP)* ausgewählt ist, wird ein Eintrag in diesem Feld ignoriert.

Domain-Suchpfad

Erleichtert dem Benutzer die Eingabe eines Domain-Namens: Gibt der Benutzer den Domain-Name gekürzt ein, ergänzt der mGuard seine Eingabe um den angegebenen Domain-Suffix, der hier unter *Domain-Suchpfad* festgelegt wird.

SNMP Information

Systemname

Ein für Verwaltungszwecke frei vergebbarer Name für den mGuard, z. B. „Hermes“, „Pluto“. (Unter SNMP: sysName)

Standort

Frei vergebbare Bezeichnung des Installationsortes, z. B. „Halle IV, Flur 3“, „Besenkammer“. (Unter SNMP: sysLocation)

Kontakt

Angabe einer für den mGuard zuständigen Kontaktperson, am besten mit Telefonnummer. (unter SNMP: sysContact)

HiDiscovery

HiDiscovery ist ein Protokoll zur Unterstützung der initialen Inbetriebnahme von neuen Netzwerkgeräten und ist im *Stealth*-Modus für das lokale Interface (LAN) des mGuard verfügbar.

Lokale HiDiscovery Unterstützung

Aktiviert

Das HiDiscovery Protokoll ist aktiviert.

Nur lesend

Das HiDiscovery Protokoll ist aktiviert, der mGuard kann jedoch nicht darüber konfiguriert werden.

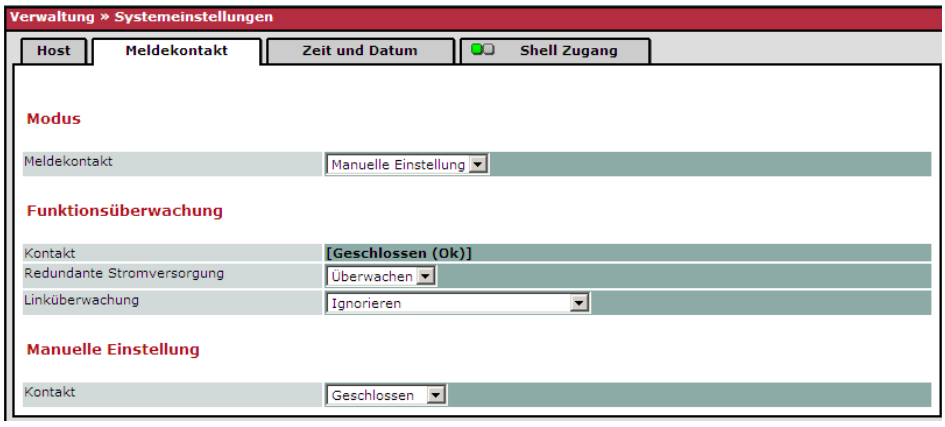
Deaktiviert

Das HiDiscovery Protokoll ist deaktiviert.

HiDiscovery Frame Durchleitung: Ja / Nein

Steht diese Option auf **Ja**, dann werden HiDiscovery Frames vom LAN-Port nach außen über den WAN-Port weitergeleitet.

Meldekontakt (nur mGuard industrial RS, EAGLE mGuard)



Der Meldekontakt ist ein Relais, mit welchem der mGuard Fehlerzustände signalisieren kann. (Siehe auch „Meldekontakt“ auf Seite 27 und Seite 33)

Modus

Meldekontakt

Der Meldekontakt kann automatisch durch die **Funktionsüberwachung** geschaltet werden (Standard), oder durch **Manuelle Einstellung**.

Siehe auch:
„mGuard industrial RS installieren“ auf Seite 24 und
„EAGLE mGuard installieren“ auf Seite 33.

Funktionsüberwachung

Kontakt

Zeigt den Zustand des Meldekontakts an. Entweder **Offen (Fehler)** oder **Geschlossen (Ok)**.

Redundante Stromversorgung

Bei **Ignorieren** hat der Zustand der Stromversorgung keinen Einfluss auf den Meldekontakt.
Bei **Überwachen** wird der Meldekontakt geöffnet, wenn eine der zwei Versorgungsspannungen ausfällt.

Linküberwachung

Überwachung des Linkstatus der Ethernetanschlüsse. Mögliche Einstellungen sind:

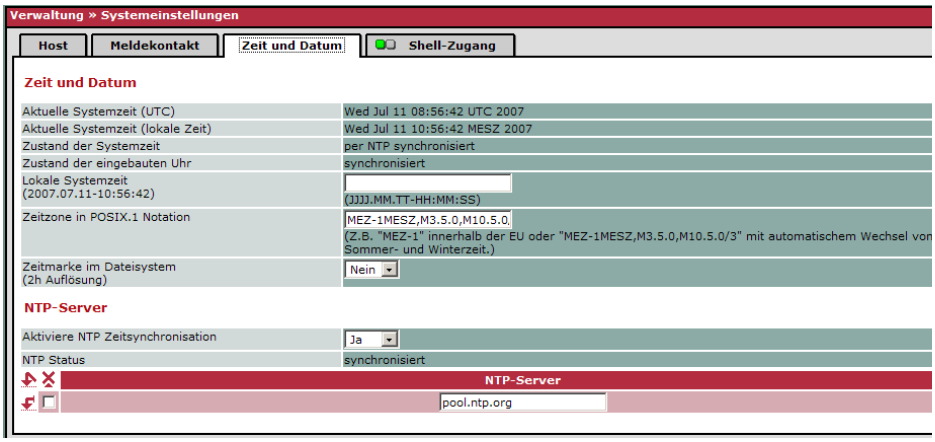
– Ignorieren
– Nur Intern (trusted) überwachen
– Nur Extern (untrusted) überwachen
– Beide überwachen

Manuelle Einstellung

Kontakt

Wenn oben unter **Meldekontakt** die Einstellung **Manuelle Einstellung** gewählt wurde, so kann man ihn hier auf **Geschlossen** oder **Offen (Alarm)** stellen.

Zeit und Datum



Zeit und Datum

Aktuelle Systemzeit (UTC)

Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC). Solange die *NTP Zeitsynchronisation* noch nicht aktiviert ist (s. u.), und *Zeitmarken im Dateisystem* deaktiviert sind, beginnt die Uhr mit dem 1. Januar 2000.

Aktuelle Systemzeit (lokale Zeit)

Anzeige: Soll die eventuell abweichende aktuelle Ortszeit angezeigt werden, müssen Sie unter *Zeitzone in POSIX.1 Notation...* (s. u.) den entsprechenden Eintrag machen.

Zustand der Systemzeit

Anzeige: Zeigt an, ob die Systemzeit des mGuards zur Laufzeit des mGuards einmal mit einer tatsächlich aktuell gültigen Zeit synchronisiert wurde. Solange hier angezeigt wird, dass die Systemzeit des mGuards nicht synchronisiert ist, führt der mGuard keine zeitgesteuerten Aktivitäten aus. Das sind Folgende:

- Zeitgesteuertes Holen der Konfiguration von einem Konfigurations-Server:
  Dies ist der Fall, wenn unter dem Menüpunkt *Verwaltung* » *Zentrale Verwaltung*, *Konfiguration holen* für die Einstellung **Schedule** die Einstellung ***Zeitgesteuert*** ausgewählt ist. (Siehe „6.2.5 Verwaltung » Konfigurationsprofile“ , „Konfiguration holen“ auf Seite 102.)
- Das Unterbrechen der Verbindung zu bestimmter Uhrzeit beim Netzwerk-Modus PPPoE:
  Dies ist der Fall, wenn unter dem Menüpunkt *Netzwerk* » *Interfaces, Allgemein* der **Netzwerk-Modus** auf PPPoE und der **Automatische Reconnect** auf Ja gesetzt ist. (Siehe „6.4.1 Netzwerk » Interfaces“ , „» Netzwerk-Modus: PPPoE“ auf Seite 125.)
- Anerkennung von Zertifikaten, solange die Systemzeit noch nicht synchronisiert ist:
  Dies ist der Fall, wenn unter dem Menüpunkt *Authentifizierung* » *Zertifikate*, *Zertifikatseinstellungen* für die Option **Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs** die Einstellung ***Warte auf Synchronisation der Systemzeit*** ausgewählt ist. (Siehe „6.5.3 Authentifizierung » Zertifikate“ , „Zertifikatseinstellungen“ auf Seite 167.)

Die Systemzeit kann durch verschiedene Ereignisse synchronisiert werden:

a) Der mGuard besitzt eine eingebaute Uhr, und diese wurde mindestens

einmal mit der aktuellen Zeit synchronisiert. Nur wenn das Feld **Zustand der eingebauten Uhr** sichtbar ist, hat der mGuard eine eingebaute Uhr. An der dortigen Anzeige lässt sich ablesen, ob sie synchronisiert ist. Eine synchronisierte eingebaute Uhr sorgt dafür, dass der mGuard auch nach einem Neustart eine synchronisierte Systemzeit hat.

b) Der Administrator hat zur Laufzeit dem mGuard die aktuelle Zeit mitgeteilt, indem er im Feld **Lokale Systemzeit** eine entsprechende Eingabe gemacht hat.

c) Der Administrator hat die Einstellung **Zeitmarke im Dateisystem** auf ***Ja*** gestellt und dem mGuard entweder per NTP (siehe unten unter *NTP-Server*) die aktuelle Systemzeit erfahren lassen oder per Eingabe in **Lokale Systemzeit** selbst eingestellt. Dann wird der mGuard auch ohne eingebaute Uhr nach einem Neustart sofort seine Systemzeit mit Hilfe des Zeitstempels synchronisieren (auch wenn sie danach eventuell noch einmal per NTP genauer eingestellt wird).

d) Der Administrator hat unten unter **NTP-Server** die NTP-Zeitsynchronisation aktiviert und die Adressen von mindestens einem NTP-Server angegeben, und der mGuard hat erfolgreich Verbindung zu mindestens einem der festgelegten NTP-Server aufgenommen. Bei funktionierendem Netzwerk geschieht dies in wenigen Sekunden nach dem Neustart. Die Anzeige im Feld **NTP Status** wechselt eventuell erheblich später erst auf "synchronisiert". Siehe dazu die Erklärung weiter unten zu **NTP-Status**.

Zustand der eingebauten Uhr

(Bei *mGuard industrial RS* und *mGuard delta*)

Der Zustand der eingebauten Uhr ist nur sichtbar, wenn der mGuard eine Uhr besitzt, die auch dann weiter läuft, wenn der mGuard nicht mit Strom versorgt wird und eingeschaltet ist. Die Anzeige gibt an, ob die Uhr einmal mit der aktuellen Zeit synchronisiert wurde. Die eingebaute Uhr wird immer dann synchronisiert, wenn die Systemzeit des mGuards synchronisiert wurde. Ist die Uhr einmal synchronisiert, wechselt ihr Zustand nur dann wieder auf "nicht synchronisiert", wenn die Firmware neu auf das Gerät aufgebracht wird (siehe Kapitel „7.3 Flashen der Firmware“ auf Seite 266) oder wenn bei ausgeschaltetem Gerät der Kondensator (mGuard industrial RS) beziehungsweise die Batterie (mGuard delta) die eingebaute Uhr zwischenzeitlich nicht mehr hinreichend unter Spannung hielt.

Lokale Systemzeit

Hier können Sie die Zeit des mGuards setzen, falls kein NTP-Server eingestellt wurde (s. u.) oder aber der NTP-Server nicht erreichbar ist.

Das Datum und die Zeit werden in dem Format JJJJ.MM.TT-HH:MM:SS angegeben:

JJJJ	Jahr
MM	Monat
TT	Tag
HH	Stunde
MM	Minute
SS	Sekunde

Zeitzone in POSIX.1 Notation...

Soll oben unter *Aktuelle Systemzeit* nicht die mittlere Greenwich-Zeit angezeigt werden sondern Ihre aktuelle Ortszeit (abweichend von der mittleren

Greenwich-Zeit), dann tragen Sie hier ein, um wieviel Stunden bei Ihnen die Zeit voraus bzw. zurück ist.

Beispiele:

In Berlin ist die Uhrzeit der mittleren Greenwich-Zeit um 1 Stunde voraus. Also tragen Sie ein: MEZ-1.

In New York geht die Uhr bezogen auf die mittlere Greenwich-Zeit um 5 Stunden nach. Also tragen Sie ein: MEZ+5.

Wichtig ist allein die Angabe -1, -2 oder +1 usw., weil nur sie ausgewertet wird; die davor stehenden Buchstaben nicht. Sie können „MEZ“ oder beliebig anders lauten, z. B. auch „UTC“.

Wünschen Sie die Anzeige der MEZ-Uhrzeit (= gültig für Deutschland) mit automatischer Umschaltung auf Sommer- bzw. Winterzeit geben Sie ein: MEZ-1MESZ,M3.5.0,M10.5.0/3

Zeitmarke im Dateisystem (2h Auflösung): Ja / Nein

Ist dieser Schalter auf **Ja** gesetzt, schreibt der mGuard alle zwei Stunden die aktuelle Systemzeit in seinen Speicher.

Folge:

Wird der mGuard aus- und wieder eingeschaltet, wird nach dem Einschalten eine Uhrzeit in diesem 2-Stunden-Zeitfenster angezeigt und nicht eine Uhrzeit am 1. Januar 2000.

NTP-Server

(NTP - Network Time Protocol) Der mGuard kann für Rechner, die an seinem LAN-Port angeschlossen sind, als NTP-Server fungieren. In diesem Fall sind die Rechner so zu konfigurieren, dass als Adresse des NTP-Servers die lokale Adresse des mGuard angegeben ist.

Wird der mGuard im *Stealth*-Modus betrieben, muss bei den Rechnern die Management-IP-Adresse des mGuard verwendet werden (sofern diese konfiguriert ist), oder es muss die IP-Adresse 1.1.1.1 als lokale Adresse des mGuard angegeben werden.

Damit der mGuard als NTP-Server fungieren kann, muss er selber das aktuelle Datum und die aktuelle Uhrzeit von einem NTP-Server (= Zeit-Server) beziehen. Dazu muss die Adresse von mindestens einem NTP-Server angegeben werden. Zusätzlich muss dieses Feature aktiviert sein.

Aktiviere NTP Zeitsynchronisation: Ja / Nein

Sobald das NTP aktiviert ist, bezieht der mGuard Datum und Uhrzeit von einem oder mehreren Zeit-Server(n) und synchronisiert sich mit ihm bzw. ihnen.

Die initiale Zeitsynchronisation kann bis zu 15 Minuten dauern. Während dieser Zeitspanne vollzieht der mGuard immer wieder Vergleiche zwischen der Zeitangabe des externen Zeit-Servers und dem eigenen "Uhrwerk", um dieses so präzise wie möglich abzustimmen. Erst dann kann der mGuard als NTP-Server für die an seiner LAN-Schnittstelle angeschlossenen Rechner fungieren und ihnen die Systemzeit liefern.

Eine initiale Zeitsynchronisation mit dem externen Zeit-Server erfolgt nach jedem Booten, es sei denn, der mGuard verfügt über eine eingebaute Uhr (*mGuard industrial RS* und *mGuard delta*). Nach der initialen Zeitsynchronisation vergleicht der mGuard regelmäßig die Systemzeit mit den Zeit-Servern. In der Regel erfolgen Nachjustierungen nur noch im Sekundenbereich.

NTP Status

Anzeige des aktuellen NTP-Status.
Gibt an, ob sich der auf dem mGuard selbst laufende NTP-Server mit hinreichender Genauigkeit mit den konfigurierten NTP-Servern synchronisiert hat.

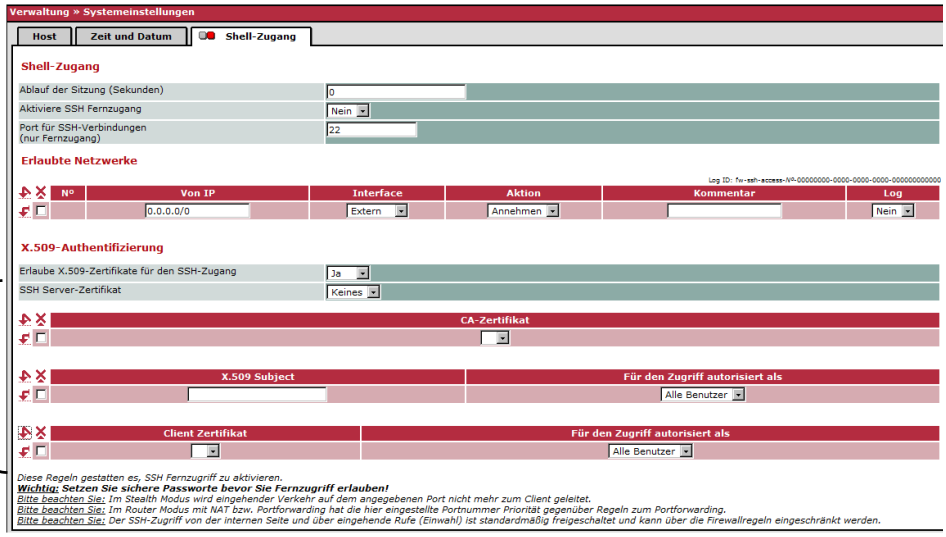
Wenn die Systemuhr des mGuards vor der Aktivierung der NTP-Zeitsynchronisation noch nie synchronisiert war, kann die Synchronisierung bis zu 15 Minuten dauern. Dennoch stellt der NTP-Server die Systemuhr des mGuards nach wenigen Sekunden auf die aktuelle Zeit um, sobald er erfolgreich einen der konfigurierten NTP-Server kontaktiert hat. Dann betrachtet der mGuard seine Systemzeit auch bereits als synchronisiert.

Nachjustierungen erfolgen in der Regel nur noch im Sekundenbereich.

NTP-Server

Geben Sie hier einen oder mehrere Zeit-Server an, von denen der mGuard die aktuelle Zeitangabe beziehen soll. Falls Sie mehrere Zeit-Server angeben, verbindet sich der mGuard automatisch mit allen, um die aktuelle Zeit zu ermitteln.

Shell-Zugang



Wird eingeblendet, wenn *Erlaube X.509-Zertifikate für den SSH-Zugang* auf **Ja** gesetzt ist

Shell-Zugang

Bei eingeschaltetem SSH Fernzugang kann der mGuard von entfernten Rechnern aus über die Kommandozeile konfiguriert werden.

Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass sichere Passwörter für *root* und *admin* festgelegt sind.

Für SSH Fernzugang machen Sie folgende Einstellungen:

Ablauf der Sitzung (Sekunden)

Gibt an, nach wie viel Zeit (in Sekunden) der Inaktivität die Sitzung automatisch beendet wird, d. h. ein automatisches Ausloggen stattfindet. Bei Einstellung von 0 (= Werkseinstellung) findet kein automatisches Beenden der Sitzung statt.

Der angegebene Wert gilt auch für Shell-Zugänge über die serielle Schnittstelle.

Aktiviere SSH Fernzugang: Ja / Nein

Wollen Sie SSH-Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**. SSH-Zugriff über *Intern* (d. h. aus dem direkt angeschlossenen LAN oder vom direkt angeschlossenen Rechner aus) ist unabhängig von der Schalterstellung möglich.

☞ Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren.

Port für SSH-Verbindungen (nur Fernzugang)

Standard: 22

Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2, VPN* und *Einwahl*. Für internen Zugriff gilt weiterhin 22.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss beim Login gegebenenfalls die Port-Nummer angeben, die hier festgelegt ist.

Beispiel:

Ist dieser mGuard über die Adresse 123.124.125.21 über das Internet zu erreichen, und ist für den Fernzugang gemäß Standard die Port-Nummer 22 festgelegt, dann muss bei der entfernten Gegenstelle im SSH-Client (z. B. PuTTY oder OpenSSH) diese Port-Nummer evtl. nicht angegeben werden.

Bei einer anderen Port-Nummer (z. B. 2222) ist diese anzugeben, z. B.:
ssh -p 2222 123.124.125.21

Erlaubte Netzwerke

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SSH-Fernzugriffs.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

⌦ Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere SSH Fernzugang** auf **Ja** steht. Weil Zugriffe von *Intern* auch möglich sind, wenn dieser Schalter auf **Nein** steht, tritt für diesen Fall eine Firewallregel, die den Zugriff von *Intern* verwehren würde, nicht in Kraft.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt beziehungsweise verboten ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise – siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263

Interface

Extern / Intern / Extern 2 / VPN / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen:
SSH-Zugriff ist erlaubt über *Intern*, *VPN* und *Einwahl*. Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

Vorsicht:

Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewallregeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen. Damit Sie sich nicht aussperren, müssen Sie eventuell gleichzeitig den Zugriff über ein anderes Interface explizit mit *Annehmen* erlauben, bevor Sie durch Klicken auf die **Übernehmen**-Schaltfläche

1. *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

die neue Einstellung in Kraft setzen. Sonst muss bei Aussperrung die Revovery-Prozedur durchgeführt werden.

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

X.509-Authentifizierung

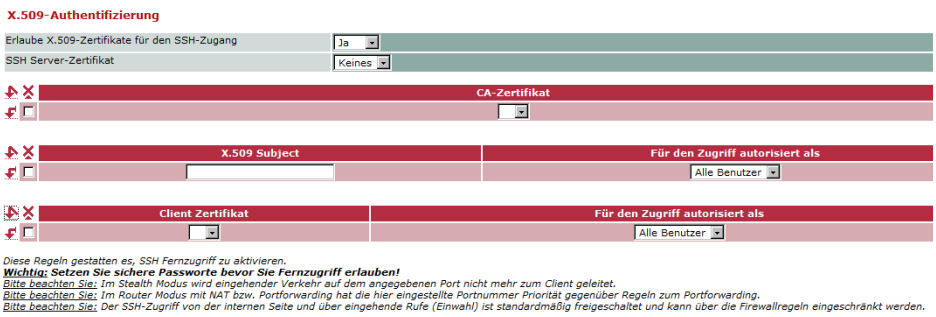
Erlaube X.509-Zertifikate für den SSH-Zugang: Ja / Nein

Bei **Nein** werden zur Authentifizierung nur die herkömmlichen Authentifizierungsverfahren (Benutzername und Passwort bzw. privater und öffentlicher Schlüssel) erlaubt, nicht das X.509-Authentifizierungsverfahren.

Bei **Ja** kann zur Authentifizierung zusätzlich zum herkömmlichen Authentifizierungsverfahren (wie es auch bei **Nein** verwendet wird) das X.509-Authentifizierungsverfahren verwendet werden.

Bei **Ja** ist festzulegen,

a) wie sich der mGuard gemäß X.509 beim SSH-Client authentisiert
b) wie der mGuard den entfernten SSH-Client gemäß X.509 authentifiziert.


X.509-Authentifizierung
Erlaube X.509-Zertifikate für den SSH-Zugang
Ja
SSH Server-Zertifikat
Keines
CA-Zertifikat
X.509 Subject
Für den Zugriff autorisiert als
Alle Benutzer
Client Zertifikat
Für den Zugriff autorisiert als
Alle Benutzer
Diese Regeln gestatten es, SSH Fernzugriff zu aktivieren.
Wichtig: Setzen Sie sichere Passworte bevor Sie Fernzugriff erlauben!
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Der SSH-Zugriff von der internen Seite und über eingehende Rufe (Einwahl) ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

→ a) ....wie sich der mGuard beim SSH-Client authentisiert

SSH Server-Zertifikat

Legt fest, wie sich der mGuard beim SSH-Client ausweist.

In der Auswahlliste eines der Maschinenzertifikate auswählen oder den Eintrag *Keines* (s. u.).

Keines:

Bei Auswahl von *Keines* authentisiert sich der SSH-Server des mGuard nicht per X.509-Zertifikat gegenüber dem SSH-Client, sondern er benutzt einen Server-Schlüssel und ist damit kompatibel mit älteren Versionen des mGuard.

Wird eines der Maschinenzertifikate ausgewählt, wird dem SSH-Client das zusätzlich angeboten, so dass dieser es sich aussuchen kann, ob er das herkömmliche Authentifizierungsverfahren oder das gemäß X.509 anwenden will.

Die Auswahlliste stellt die Maschinenzertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen worden sind - siehe in diesem Handbuch unter „Authentifizierung » Zertifikate“ auf Seite 163.

→ b) ....wie der mGuard den SSH-Client authentifiziert

Nachfolgend wird festgelegt, wie der mGuard die Authentizität des SSH-Clients prüft.

Die Tabelle unten zeigt, welche Zertifikate dem mGuard zur Authentifizierung des SSH-Clients zur Verfügung stehen müssen, wenn der SSH-Client bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt:

- ein von einer CA signiertes Zertifikat
- ein selbst signiertes Zertifikat
  Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „6.5.3 Authentifizierung » Zertifikate“ auf Seite 163.

Authentifizierung bei SSH

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von:	⇕	⇕
	Alle CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellenzertifikate, wenn als Filter verwendet	Gegenstellenzertifikat

Gemäß dieser Tabelle sind nachfolgend die Zertifikate zur Verfügung zu stellen, die der mGuard zur Authentifizierung des jeweiligen SSH-Clients heranziehen muss.

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind. Siehe „6.5.3 Authentifizierung » Zertifikate“ auf Seite 163.

⌦ Ist unter Menüpunkt *Authentifizierung » Zertifikate, Zertifikatseinstellungen* die Verwendung von Sperrlisten (= CRL-Prüfung) aktiviert, wird jedes von einer CA signierte Zertifikat, das SSH-Clients "vorzeigen", auf Sperrung geprüft.

CA-Zertifikat

Die Konfiguration ist nur dann erforderlich, wenn der SSH-Client ein von einer CA signiertes Zertifikat vorzeigt.

Es sind alle CA-Zertifikate zu konfigurieren, die der mGuard benötigt, um mit den von SSH-Clients vorgezeigten Zertifikaten jeweils die Kette bis zum jeweiligen Root-CA-Zertifikat zu bilden.

Die Auswahlliste stellt die CA-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen worden sind.

X.509 Subject

Ermöglicht die Filtersetzung in Bezug auf den Inhalt des Feldes *Subject* im Zertifikat, das vom SSH-Client vorgezeigt wird. Dadurch ist es möglich, den Zugriff von SSH-Clients, die der mGuard auf Grundlage von Zertifikatsprüfungen im Prinzip akzeptieren würde, wie folgt zu beschränken bzw. freizugeben:

- Beschränkung auf bestimmte *Subjects* (d. h. Personen) und/oder auf *Subjects*, die bestimmte Merkmale (Attribute) haben

oder

- Freigabe für alle Subjects

(Siehe dazu auch im Glossar unter „Subject, Zertifikat“.)

Das Feld *X.509 Subject* darf nicht leer bleiben.

Freigabe für alle Subjects (d. h. Personen):
Mit * (Sternchen) im Feld *X.509 Subject* legen Sie fest, dass im vom SSH-Client vorgezeigten Zertifikat beliebige Subject-Einträge erlaubt sind. Dann ist es überflüssig, das im Zertifikat jeweils angegebene Subject zu kennen oder festzulegen.

Beschränkung auf bestimmte Subjects (d. h. Personen) und/oder auf Subjects, die bestimmte Merkmale (Attribute) haben:
Im Zertifikat wird der Zertifikatsinhaber im Feld *Subject* angegeben, dessen Eintrag sich aus mehreren Attributen zusammensetzt. Diese Attribute werden entweder als Object Identifier ausgedrückt (z. B.: 132.3.7.32.1) oder, geläufiger, als Buchstabenkürzel mit einem entsprechenden Wert.
Beispiel: CN=Max Muster, O=Fernwartung GmbH, C=DE

Sollen bestimmte Attribute des Subjects ganz bestimmte Werte haben, damit der mGuard den SSH-Client akzeptiert, muss das entsprechend spezifiziert werden. Die Werte der anderen Attribute, die beliebig sein können, werden dann durch das Wildcard * (Sternchen) angegeben.
Beispiel: CN=*, O=*, C=DE (mit o. ohne Leerzeichen zwischen Attributen)

Bei diesem Beispiel müsste im Zertifikat im Subject das Attribut "C=DE" stehen. Nur dann würde der mGuard den Zertifikatsinhaber (= Subject) als Kommunikationspartner akzeptieren. Die anderen Attribute könnten in den zu filternden Zertifikaten beliebige Werte haben.

☞ Wird ein Subject-Filter gesetzt, muss zwar die Anzahl, nicht aber die Reihenfolge der angegebenen Attribute mit der übereinstimmen, wie sie

in den Zertifikaten gegeben ist, auf die der Filter angewendet werden soll.
Auf Groß- und Kleinschreibung ist zu achten.

☞ Es können mehrere Filter gesetzt werden, die Reihenfolge ist irrelevant.

Für den Zugriff autorisiert als: Alle Benutzer / root / admin / netadmin / audit

Zusätzlicher Filter, der festlegt, dass der SSH-Client für eine bestimmte Verwaltungsebene autorisiert sein muss, um Zugriff zu erhalten.

Erläuterung:

Der SSH-Client zeigt bei Verbindungsaufnahme nicht nur sein Zertifikat vor, sondern gibt auch den Systembenutzer an, für den die SSH-Sitzung eröffnet werden soll (*root, admin, netadmin, audit*). Nur wenn diese Angabe mit der übereinstimmt, die hier festgelegt wird, erhält er Zugriff.

Mit der Einstellung *Alle Benutzer* ist der Zugriff für jeden der vorgenannten Systembenutzer möglich.

☞ Die Einstellmöglichkeiten *netadmin* und *audit* beziehen sich auf Zugriffsrechte mit dem Innominate Device Manager.

Client Zertifikat

Die Konfiguration ist in den folgenden Fällen erforderlich:

- SSH-Clients zeigen jeweils ein selbst signiertes Zertifikat vor.
- SSH-Clients zeigen jeweils ein von einer CA signiertes Zertifikat vor. Es soll eine Filterung erfolgen: Zugang erhält nur der, dessen Zertifikats-Kopie im mGuard als Gegenstellenzertifikat installiert ist und in dieser Tabelle dem mGuard als *Client-Zertifikat* zur Verfügung gestellt wird. Dieser Filter ist dem *Subject*-Filter darüber nicht nachgeordnet, sondern ist auf gleicher Ebene angesiedelt, ist also dem *Subject*-Filter mit einem logischen ODER beigeordnet.

Der Eintrag in diesem Feld legt fest, welches Gegenstellenzertifikat der mGuard heranziehen soll, um die Gegenstelle, den SSH-Client, zu authentifizieren.

Dazu in der Auswahlliste eines der Gegenstellenzertifikate auswählen.

Die Auswahlliste stellt die Gegenstellenzertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen worden sind.

Für den Zugriff autorisiert als: Alle Benutzer / root / admin / netadmin / audit

Filter, der festlegt, dass der SSH-Client für eine bestimmte Verwaltungsebene autorisiert sein muss, um Zugriff zu erhalten.

Erläuterung:

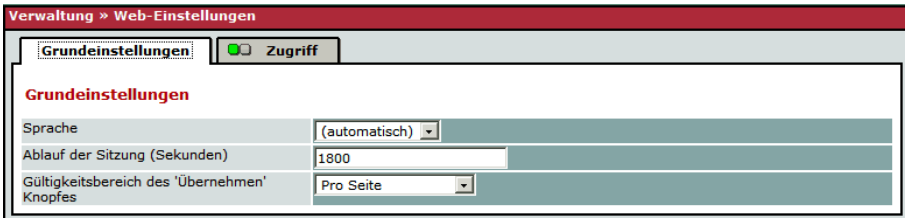
Der SSH-Client zeigt bei Verbindungsaufnahme nicht nur sein Zertifikat vor, sondern gibt auch den Systembenutzer an, für den die SSH-Sitzung eröffnet werden soll (*root, admin, netadmin, audit*). Nur wenn diese Angabe mit der übereinstimmt, die hier festgelegt wird, erhält er Zugriff.

Mit der Einstellung *Alle Benutzer* ist der Zugriff für jeden der vorgenannten Systembenutzer möglich.

☞ Die Einstellmöglichkeiten *netadmin* und *audit* beziehen sich auf Zugriffsrechte mit dem Innominate Device Manager.

6.2.2 Verwaltung » Web Einstellungen

Grundeinstellungen



Grundeinstellungen

Sprache

Ist in der Sprachauswahlliste **(Automatisch)** ausgewählt, übernimmt das Gerät die Spracheinstellung aus dem Browser des Rechners.

Ablauf der Sitzung (Sekunden)

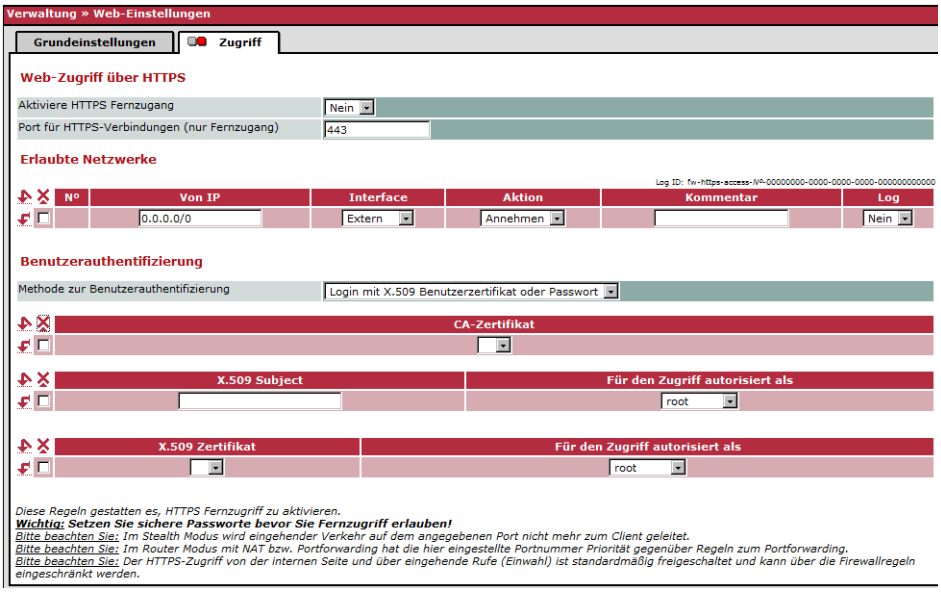
Sekunden der Inaktivität, nach denen der Benutzer von der Web-Schnittstelle des mGuard automatisch abgemeldet wird. Mögliche Werte: 15 bis 86400 (= 24 Stunden)

Gültigkeitsbereich des 'Übernehmen' Knopfes

Mit **Pro Seite** wird festgelegt, dass Sie auf jeder Seite, auf der Sie Änderungen vorgenommen haben, jeweils die Schaltfläche **Übernehmen** zu klicken haben, damit die Einstellungen vom mGuard übernommen und in Kraft gesetzt werden.

Mit **Seitenübergreifend** wird festgelegt, dass Sie nach Vornahme von Änderungen auf mehren Seiten nur einmalig **Übernehmen** klicken müssen.

Zugriff


Verwaltung » Web-Einstellungen
Grundeinstellungen
Zugriff
Web-Zugriff über HTTPS
Aktiviere HTTPS Fernzugang
Nein
Port für HTTPS-Verbindungen (nur Fernzugang)
443
Erlaubte Netzwerke
Nº
Von IP
Interface
Aktion
Kommentar
Log
0.0.0.0/0
Extern
Annehmen
Nein
Benutzerauthentifizierung
Methode zur Benutzerauthentifizierung
Login mit X.509 Benutzerzertifikat oder Passwort
CA-Zertifikat
X.509 Subject
Für den Zugriff autorisiert als
root
X.509 Zertifikat
Für den Zugriff autorisiert als
root
Diese Regeln gestatten es, HTTPS Fernzugriff zu aktivieren.
Wichtig: Setzen Sie sichere Passworte bevor Sie Fernzugriff erlauben!
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Der HTTPS-Zugriff von der internen Seite und über eingehende Rufe (Einwahl) ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Nur eingeblendet bei *Login mit X.509-Benutzerzertifikat*

Bei eingeschaltetem Web-Zugriff per HTTPS-Protokoll kann der mGuard über seine Web-basierte Administratoroberfläche von entfernten Rechnern aus konfiguriert werden. Das heißt, auf dem entfernten Rechner wird der Browser benutzt, um den mGuard zu konfigurieren.

Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass sichere Passwörter für *root* und *admin* festgelegt sind.

Um HTTPS Fernzugang zu ermöglichen, machen Sie nachfolgende Einstellungen:

Web-Zugriff über HTTPS

Aktiviere HTTPS Fernzugang: Ja / Nein

Wollen Sie HTTPS-Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**. HTTPS-Fernzugriff über *Intern* (d. h. aus dem direkt angeschlossenen LAN oder vom direkt angeschlossenen Rechner aus) ist unabhängig von dieser Schalterstellung möglich.

☞ Um Zugriffsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren. Zusätzlich müssen gegebenenfalls unter **Benutzerauthentifizierung** die Authentifizierungsregeln gesetzt werden.

Port für HTTPS-Verbindungen (nur Fernzugang)

Standard: 443

Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2, VPN* und *Einwahl*. Für internen Zugriff gilt weiterhin 443.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe hinter der IP-Adresse gegebenenfalls die Port-Nummer angeben, die hier festgelegt ist.

Beispiel:

Ist dieser mGuard über die Adresse 123.124.125.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser diese Port-Nummer nicht hinter der Adresse angegeben werden.

Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B.: https://123.124.125.21:442/

HINWEIS:

- Der mGuard authentisiert sich bei der Gegenstelle, in diesem Fall dem Browser des Bedieners, mit einem selbst signiertem Maschinenzertifikat. Es handelt sich um ein von Innominate einmalig für jeden mGuard ausgestelltes Zertifikat. D. h. jeder mGuard wird mit einem einzigartigen selbstunterzeichneten Maschinenzertifikat ausgeliefert.

Erlaubte Netzwerke

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines HTTPS-Fernzugriffs.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

- Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere HTTPS Fernzugang** auf **Ja** steht. Weil Zugriffe von *Intern* auch möglich sind, wenn dieser Schalter auf **Nein** steht, tritt für diesen Fall eine Firewallregel, die den Zugriff von *Intern* verwehren würde, nicht in Kraft.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt beziehungsweise verboten ist.

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise – siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263

Interface

Extern / Intern / Extern 2 / VPN / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen:

HTTPS-Zugriff ist erlaubt über *Intern, VPN* und *Einwahl*. Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

Vorsicht:

1. *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewallregeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen. Damit Sie sich nicht aussperren, müssen Sie eventuell gleichzeitig den Zugriff über ein anderes Interface explizit mit *Annehmen* erlauben, bevor Sie durch Klicken auf die **Übernehmen**-Schaltfläche die neue Einstellung in Kraft setzen. Sonst muss bei Aussperrung die Revovery-Prozedur durchgeführt werden.

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

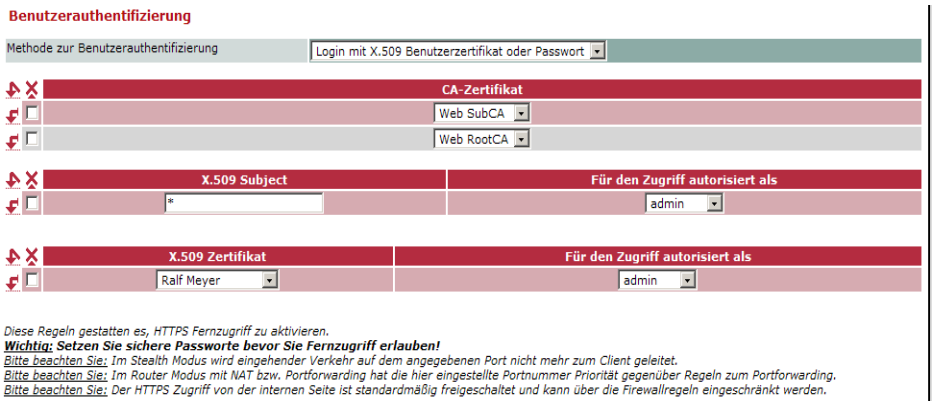
Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Benutzerauthentifizierung


Benutzerauthentifizierung
Methode zur Benutzerauthentifizierung
Login mit X.509 Benutzerzertifikat oder Passwort
CA-Zertifikat
Web SubCA
Web RootCA
X.509 Subject
Für den Zugriff autorisiert als
*
admin
X.509 Zertifikat
Für den Zugriff autorisiert als
Ralf Meyer
admin
Diese Regeln gestatten es, HTTPS Fernzugriff zu aktivieren.
Wichtig: Setzen Sie sichere Passworte bevor Sie Fernzugriff erlauben!
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Der HTTPS Zugriff von der internen Seite ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Methode zur Benutzerauthentifizierung

Legt fest, wie der lokale mGuard die entfernte Gegenstelle authentifiziert

Login mit Passwort

Legt fest, dass sich der aus der Ferne zugreifende Bediener des mGuard mit Angabe seines Passwortes beim mGuard anmelden muss. Das Passwort ist festgelegt unter Menü *Authentifizierung » Lokale Benutzer* - siehe in diesem Handbuch unter „Authentifizierung » Lokale Benutzer“ auf Seite 158.

Je nach dem, mit welcher Benutzerkennung der Bediener sich anmeldet (User- oder Administrator-Passwort), hat er entsprechende Rechte, den mGuard zu bedienen bzw. zu konfigurieren.

Login mit X.509 Benutzerzertifikat oder Passwort

Legt Folgendes fest:

1 Die Benutzerauthentifizierung erfolgt per Login mit Passwort (siehe oben).

ODER

2 Der Browser des Benutzers authentisiert sich mit Hilfe eines X.509-Zertifikates und einem dazugehörigen privaten Schlüssel. Dazu sind unten weitere Angaben zu machen.

Ob 1 oder 2 zur Anwendung kommt, hängt vom Web-Browser des von entfernt zugreifenden Benutzers ab. Option 2 kommt dann zur Anwendung, wenn der Web-Browser dem mGuard ein Zertifikat anbietet.

Login nur mit X.509 Benutzerzertifikat

Der Browser des Benutzers muss sich sich mit Hilfe eines X.509-Zertifikates und dem zugehörigen privaten Schlüssel authentisieren. Dazu sind unten weitere Angaben zu machen.

☞ Bevor Sie die Einstellung ***Login nur mit X.509 Benutzerzertifikat*** in Kraft setzen, unbedingt erst die Einstellung ***Login mit X.509 Benutzerzertifikat oder Passwort*** wählen und testen. Erst wenn sichergestellt ist, dass diese Einstellung funktioniert, auf ***Login nur mit X.509 Benutzerzertifikat*** umstellen. Sonst könnte es passieren, dass Sie sich selbst aussperren!
Diese Vorsichtsmaßnahme unbedingt immer dann treffen, wenn unter **Benutzerauthentifizierung** Einstellungen geändert werden.

Ist als **Methode der Benutzerauthentifizierung** festgelegt:

- Login nur mit X.509 Benutzerzertifikat

ODER

- Login mit X.509 Benutzerzertifikat oder Passwort:

Dann wird nachfolgend festgelegt, wie der mGuard den aus der Ferne zugreifenden Benutzer gemäß X.509 zu authentifizieren hat.

Die Tabelle unten zeigt, welche Zertifikate dem mGuard zur Authentifizierung des per HTTPS zugreifenden Benutzers zur Verfügung stehen müssen, wenn der Benutzer bzw. dessen Browser bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt:

- ein von einer CA signiertes Zertifikat
- ein selbst signiertes Zertifikat

Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „6.5.3 Authentifizierung » Zertifikate“ auf Seite 163.

X.509-Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert***	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von:		
	Alle CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigtem Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellenzertifikate, wenn als Filter verwendet	Gegenstellenzertifikat

* Die Gegenstelle kann zusätzlich Sub-CA-Zertifikate anbieten. In diesem Fall kann der mGuard mit den angebotenen CA-Zertifikaten und den bei ihm selber konfigurierten CA-Zertifikaten die Vereinigungsmenge bilden, um die Kette zu bilden. Auf jeden Fall muss aber das zugehörige Root-Zertifikat auf dem mGuard zur Verfügung stehen.

Gemäß dieser Tabelle sind nachfolgend die Zertifikate zur Verfügung zu stellen, die der mGuard benutzen muss, um einen von entfernt per HTTPS zugreifenden Benutzer bzw. dessen Browser zu authentifizieren.

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind. Siehe „6.5.3 Authentifizierung » Zertifikate“ auf Seite 163.

⌦ Ist unter Menüpunkt *Authentifizierung » Zertifikate, Zertifikatseinstellungen* die Verwendung von Sperrlisten (= CRL-Prüfung) aktiviert, wird jedes von einer CA signierte Zertifikat, das von entfernt zugreifende Benutzer "vorzeigen", auf Sperrung geprüft.

CA-Zertifikat

Die Konfiguration ist nur erforderlich, wenn der Benutzer, der per HTTPS zugreift, ein von einer CA signiertes Zertifikat vorzeigt.

Es sind alle CA-Zertifikate zu konfigurieren, die der mGuard benötigt, um mit den von Benutzern vorgezeigten Zertifikaten jeweils die Kette bis zum jeweiligen Root-CA-Zertifikat zu bilden.

Sollte der Browser des aus der Ferne zugreifenden Benutzers zusätzlich CA-Zertifikate anbieten, die zur Bildung dieser Kette beitragen, dann ist es nicht notwendig, dass genau diese CA-Zertifikate beim mGuard installiert und an dieser Stelle referenziert werden. Es muss aber auf jeden Fall das zugehörige Root-CA-Zertifikat beim mGuard installiert und zur Verfügung gestellt (= referenziert) sein.

☞ Bei Auswahl anzuwendender CA-Zertifikate oder bei der Änderung der Auswahl oder Filtersetzung sollten Sie vor Inkraftsetzen der (neuen) Einstellung unbedingt erst die Einstellung ***Login mit X.509 Benutzerzertifikat oder Passwort*** als *Methode zur Benutzerauthentifizierung*

wählen und testen. Erst wenn sichergestellt ist, dass diese Einstellung funktioniert, auf ***Login nur mit X.509 Benutzerzertifikat*** umstellen.
Sonst könnte es passieren, dass Sie sich selbst aussperren!
Diese Vorsichtsmaßnahme unbedingt immer dann treffen, wenn unter **Benutzerauthentifizierung** Einstellungen geändert werden.

X.509 Subject

Ermöglicht die Filtersetzung in Bezug auf den Inhalt des Feldes *Subject* im Zertifikat, das vom Benutzer vorgezeigt wird. Dadurch ist es möglich, den Zugriff von Benutzern, die der mGuard auf Grundlage von Zertifikatsprüfungen im Prinzip akzeptieren würde, wie folgt zu beschränken bzw. freizugeben:

- Beschränkung auf bestimmte *Subjects* (d. h. Personen) und/oder auf *Subjects*, die bestimmte Merkmale (Attribute) haben

oder

- Freigabe für alle Subjects

(Siehe dazu auch im Glossar unter „Subject, Zertifikat“.)

Das Feld *X.509 Subject* darf nicht leer bleiben.

Freigabe für alle Subjects (d. h. Personen):
Mit * (Sternchen) im Feld *X.509 Subject* legen Sie fest, dass im vom HTTPS-Client vorgezeigten Zertifikat beliebige Subject-Einträge erlaubt sind. Dann ist es überflüssig, das im Zertifikat jeweils angegebene Subject zu kennen oder festzulegen.

Beschränkung auf bestimmte Subjects (d. h. Personen) und/oder auf Subjects, die bestimmte Merkmale (Attribute) haben:
Im Zertifikat wird der Zertifikatsinhaber im Feld *Subject* als Wesenheit angegeben, die sich aus mehreren Attributen zusammensetzt. Diese Attribute werden entweder als Object Identifier ausgedrückt (z. B.: 132.3.7.32.1) oder, geläufiger, als Buchstabenkürzel mit einem entsprechenden Wert.
Beispiel: CN=Max Muster, O=Fernwartung GmbH, C=DE

Sollen bestimmte Attribute des Subjects ganz bestimmte Werte haben, damit der mGuard den Benutzer akzeptiert, muss das entsprechend spezifiziert werden. Die Werte der anderen Attribute, die beliebig sein können, werden dann durch das Wildcard * (Sternchen) angegeben.
Beispiel: CN=*, O=*, C=DE (mit o. ohne Leerzeichen zwischen Attributen)

Bei diesem Beispiel müsste im Zertifikat im Subject das Attribut "C=DE" stehen. Nur dann würde der mGuard den Zertifikatsinhaber (= Subject) als Kommunikationspartner akzeptieren. Die anderen Attribute könnten in den zu filternden Zertifikaten beliebige Werte haben.

☞ Wird ein Subject-Filter gesetzt, muss zwar die Anzahl, nicht aber die Reihenfolge der angegebenen Attribute mit der übereinstimmen, wie sie in den Zertifikaten gegeben ist, auf die der Filter angewendet werden soll.
Auf Groß- und Kleinschreibung ist zu achten.

☞ Es können mehrere Filter gesetzt werden. Auf die Reihenfolge ist zu achten! Denn bei HTTPS gibt der Browser des zugreifenden Benutzers nicht an, mit welchen Benutzer- bzw. Administratorrechten dieser sich anmeldet. Diese Rechtevergabe erfolgt bei der Filtersetzung hier (unter

"Für den Zugriff autorisiert"). Das hat folgende Konsequenz: Gibt es mehrere Filter, die einen bestimmten Benutzer "durchlassen", tritt der erste Filter in Kraft. Und der Benutzer erhält das Zugriffsrecht, das ihm in diesem Filter zugesprochen wird. Und das könnte sich unterscheiden von Zugriffsrechten, die ihm in weiter unten stehenden Filtern zugeordnet sind.

☞ Sind nachfolgend in der Tabelle mit der Spalte **X.509 Zertifikat** Gegenstellenzertifikate als Filter konfiguriert, dann haben diese Filter Vorrang gegenüber den Filtersetzungen hier.

Für den Zugriff autorisiert als: root / admin / netadmin / audit / user

Legt fest, welche Benutzer- bzw. Administratorrechte dem aus der Ferne zugreifenden Bediener eingeräumt werden.

Für eine Beschreibung der Berechtigungsstufen *root, admin* und *user* siehe „Authentifizierung » Lokale Benutzer“ auf Seite 158.

Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte bei Zugriffen mit dem Innominate Device Manager.

X.509 Zertifikat

Die Konfiguration ist in den folgenden Fällen erforderlich:

- Von entfernt zugreifende Benutzer zeigen jeweils ein selbst signiertes Zertifikat vor.
- Von entfernt zugreifende Benutzer zeigen jeweils ein von einer CA signiertes Zertifikat vor. Es soll eine Filterung erfolgen: Zugang erhält nur der, dessen Zertifikats-Kopie im mGuard als Gegenstellenzertifikat installiert ist und in dieser Tabelle dem mGuard als *X.509 Zertifikat* zur Verfügung gestellt wird.
  Dieser Filter hat Vorrang gegenüber dem *Subject*-Filter in der Tabelle darüber, sofern verwendet.

Der Eintrag in diesem Feld legt fest, welches Gegenstellenzertifikat der mGuard heranziehen soll, um die Gegenstelle, den Browser des von entfernt zugreifenden Benutzers, zu authentifizieren.

Dazu in der Auswahlliste eines der Gegenstellenzertifikate auswählen.

Die Auswahlliste stellt die Gegenstellenzertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen worden sind.

Für den Zugriff autorisiert als: root / admin / netadmin / audit / user

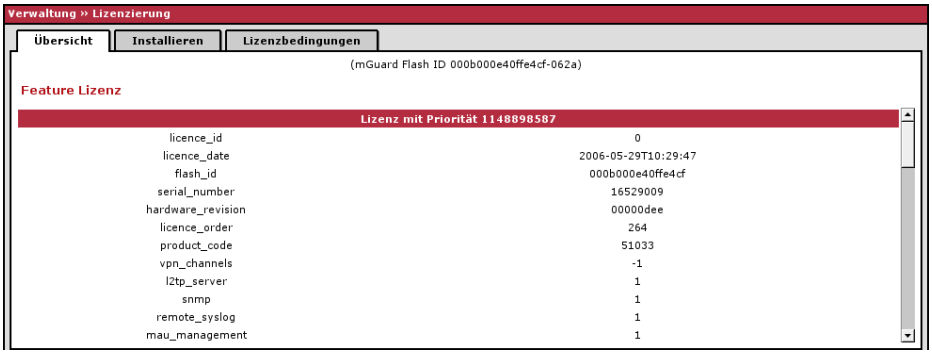
Legt fest, welche Nutzer- bzw. Administratorrechte dem aus der Ferne zugreifenden Bediener eingeräumt werden.

Für eine Beschreibung der Berechtigungsstufen *root, admin* und *user* siehe „Authentifizierung » Lokale Benutzer“ auf Seite 158.

Die Berechtigungsstufen *netadmin* und *audit* beziehen sich auf Zugriffsrechte mit dem Innominate Device Manager.

6.2.3 Verwaltung » Lizenzierung

Übersicht



⌦ Ab Version 5.0 des mGuard bleiben Lizenzen auch nach Flashen der Firmware installiert.

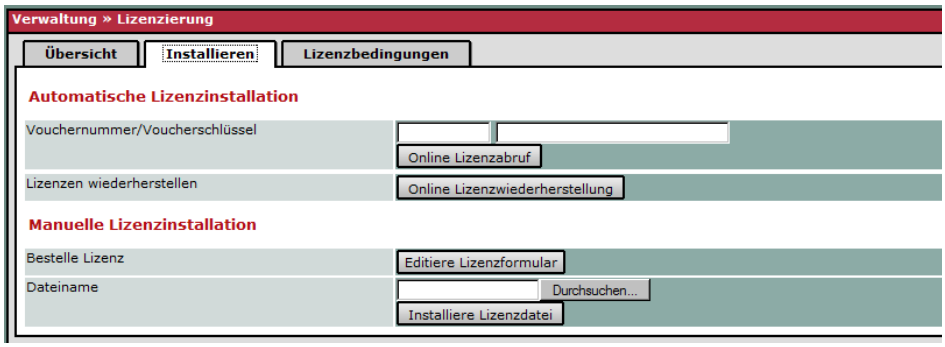
Beim Flashen von Geräten mit älteren Firmware-Versionen auf Versionen 5.0.0 oder später werden weiterhin Lizenzen gelöscht. Dann muss vor dem Flashen erst die Lizenz für die Nutzung des neuen Updates erworben werden, damit beim Flashen die erforderliche Lizenz-Datei zur Verfügung steht.

Das gilt für Major-Release Upgrades, also z. B. bei einem Upgrade von Version 4.x.y zu Version 5.x.y zu Version 6.x.y usw. Siehe „Flashen der Firmware“ auf Seite 266.

Feature-Lizenz

Zeigt an, welche Funktionen die eingespielten mGuard-Lizenzen beinhalteten, z. B. die Anzahl der ermöglichten VPN-Tunnel, ob Remote Logging unterstützt wird, usw.

Installieren



Sie können nachträglich Ihre erworbene mGuard-Lizenz um weitere Funktionen ergänzen. Im Voucher, den Sie beim Kauf des mGuard erhalten oder zusätzlich erworben haben, finden Sie eine Voucher-Seriennummer und einen Voucher-Schlüssel. Damit können Sie

1. die erforderliche Feature-Lizenzdatei anfordern und dann
2. die Lizenzdatei, die Sie daraufhin erhalten, installieren.

Automatische Lizenzinstallation

Vouchernummer/Voucherschlüssel

Geben Sie hier die Seriennummer, die auf dem Voucher aufgedruckt ist, sowie den dazugehörigen Voucherschlüssel ein, und klicken Sie anschließend **Online Lizenzabruf**.

Folge:

Der mGuard baut nun eine Verbindung über das Internet auf und installiert bei einem gültigen Voucher die zugehörige Lizenz auf dem mGuard.

Lizenzen wiederherstellen

Kann benutzt werden, falls die im Guard installierten Lizenzen gelöscht wurde. Klicken Sie dazu auf die Schaltfläche **Online Lizenzwiederherstellung**.

Dann werden die Lizenzen, die zuvor für diesen mGuard ausgestellt waren, über das Internet vom Server geholt und installiert.

Manuelle Lizenzinstallation

Lizenz bestellen

Nach Klicken auf die Schaltfläche **Editiere Lizenzformular** wird über eine Internet-Verbindung ein Formular bereit gestellt, über das Sie die gewünschte Lizenz bestellen können und in deren Felder Sie die folgenden Informationen eingeben:

Voucher Serial Number: Die Seriennummer, die auf Ihrem Voucher gedruckt ist

Voucher Key: Der Voucherschlüssel auf ihrem Voucher

Flash Id: Wird automatisch vorausgefüllt

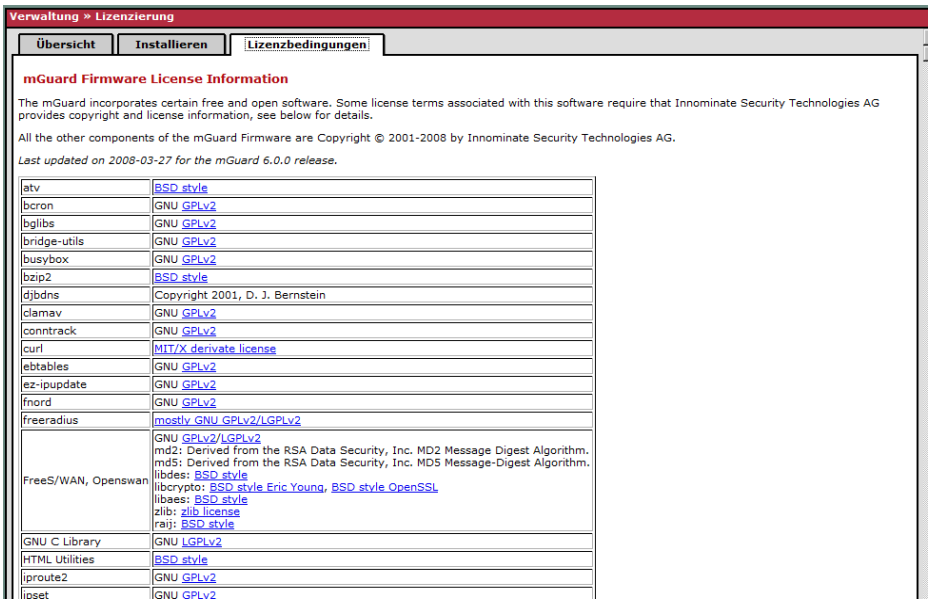
Nach dem Absenden des Formulars wird die Lizenzdatei zum Herunterladen bereitgestellt und kann mit einem weiteren Schritt im mGuard installiert werden.

Lizenzdatei installieren

Um eine Lizenz einzuspielen, speichern Sie zunächst die Lizenz-Datei als separate Datei auf Ihrem Rechner und gehen dann wie folgt vor:

1. Hinter dem Feld *Dateiname* die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und öffnen, so dass ihr Pfad- bzw. Dateiname im Feld *Dateiname* angezeigt wird.
2. Dann die Schaltfläche **Installiere Lizenzdatei** klicken.

Lizenzbedingungen



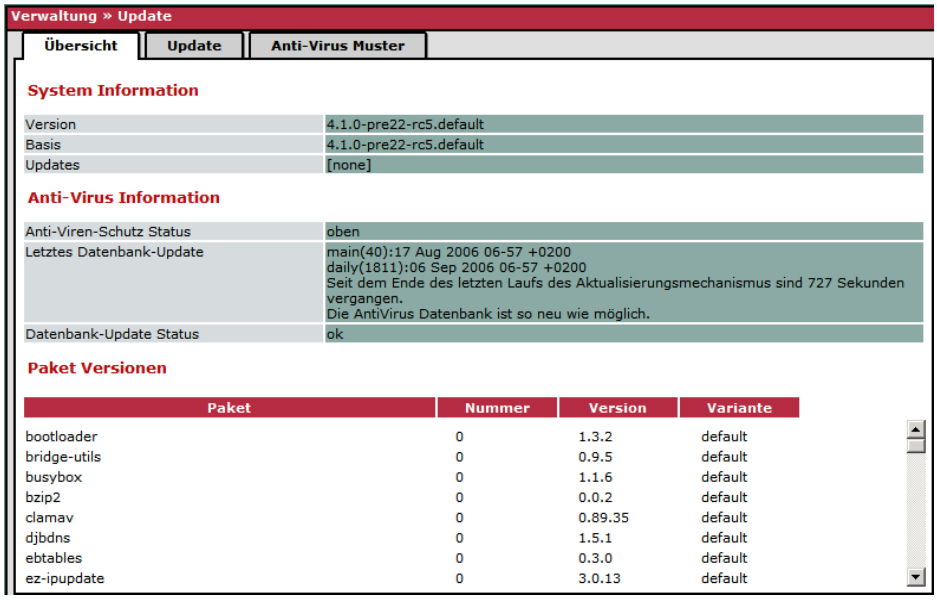
Listet die Lizenzen der Fremd-Software auf, die im mGuard verwendet wird. Es handelt sich meistens um Open-Source-Software.

6.2.4 Verwaltung » Update

⌦ Ab Version 5.0.0 der mGuard-Firmware muss vor der Installation eines Major-Release-Upgrades (z. B. von Version 4.x.y auf 5.x.y oder von Version 5.x.y auf Version 6.x.y) für das betreffende Gerät erst eine Lizenz erworben werden. Die Lizenz muss vor der Durchführung des Firmware-Updates auf dem Gerät installiert werden (siehe „6.2.3 Verwaltung » Lizenzierung“ , „Installieren“ auf Seite 83)
Minor-Release-Upgrades (bedeutet: gleichbleibende Hauptversion, z. B. innerhalb von 5.x.y) können bis auf Weiteres ohne Lizenz installiert werden.

⌦ Ab Firmware-Version 5.0 des mGuard bleiben Lizenzen auch nach Flashen der Firmware installiert.

Übersicht



Sie können die erfolgreiche Freischaltung des Virenfilters überprüfen.
Die Information über das Ablaufdatum Ihrer Anti-Virus-Lizenz: Siehe „Verwaltung » Lizenzierung“ auf Seite 82.

System Information

Version

Die aktuelle Software-Version des mGuard.

Basis

Die Software-Version, mit der dieser mGuard ursprünglich geflasht wurde.

Updates

Liste der Updates, die zur Basis hinzu installiert worden sind.

Anti-Virus Information

Anti-Viren-Schutz Status

Hier können Sie den Status der Scan-Engine überprüfen. Wenn die Überwachung für mindestens ein Protokoll aktiviert ist, wird hier der Status **oben** angezeigt.

Letztes Datenbank-Update

Es werden die Versionsnummern und das Erstellungsdatum der Virensignaturen angezeigt.

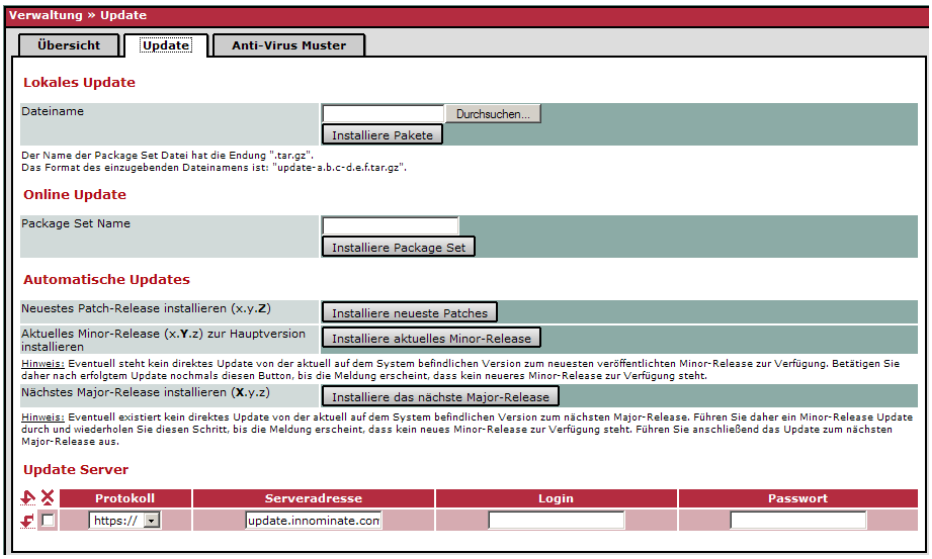
Datenbank-Update Status

Hier wird angezeigt, ob die Datenbank-Aktualisierung aktiviert ist, ob gerade ein Datenbank-Update durchgeführt wird oder ob die Aktualisierung wegen einer abgelaufenen Anti-Virus-Lizenz gesperrt ist.

Paket Versionen

Listet die einzelnen Software-Module des mGuard auf. Gegebenenfalls für Supportzwecke interessant.

Update


Verwaltung » Update
Übersicht
Update
Anti-Virus Muster
Lokales Update
Dateiname
Durchsuchen...
Installiere Pakete
Der Name der Package Set Datei hat die Endung ".tar.gz".
Das Format des einzugebenden Dateinamens ist: "update-a.b.c-d.e.f.tar.gz".
Online Update
Package Set Name
Installiere Package Set
Automatische Updates
Neuestes Patch-Release installieren (x.y.Z)
Installiere neueste Patches
Aktuelles Minor-Release (x.Y.z) zur Hauptversion installieren
Installiere aktuelles Minor-Release
Hinweis: Eventuell steht kein direktes Update von der aktuell auf dem System befindlichen Version zum neuesten veröffentlichten Minor-Release zur Verfügung. Betätigen Sie daher nach erfolgtem Update nochmals diesen Button, bis die Meldung erscheint, dass kein neueres Minor-Release zur Verfügung steht.
Nächstes Major-Release installieren (X.y.z)
Installiere das nächste Major-Release
Hinweis: Eventuell existiert kein direktes Update von der aktuell auf dem System befindlichen Version zum nächsten Major-Release. Führen Sie daher ein Minor-Release Update durch und wiederholen Sie diesen Schritt, bis die Meldung erscheint, dass kein neues Minor-Release zur Verfügung steht. Führen Sie anschließend das Update zum nächsten Major-Release aus.
Update Server
Protokoll
Serveradresse
Login
Passwort
https://
update.innominate.com

Um ein Firmware-Update durchzuführen, gibt es zwei Möglichkeiten:

– Sie haben die aktuelle Package-Set-Datei auf Ihrem Rechner (der Dateiname hat die Endung „.tar.gz“) und Sie führen ein lokales Update durch.

ODER

– Sie laden die Package-Set-Datei per Internet vom Update Server herunter und installieren dann die Pakete.

⌦ Abhängig von der Größe des Updates, kann dieses mehrere Minuten dauern.

⌦ Falls zum Abschluss des Updates ein Neustart erforderlich sein sollte, werden Sie durch eine Nachricht darauf hingewiesen.

⌦ **Sie dürfen während des Updates auf keinen Fall die Stromversorgung des mGuard unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden können.**

⌦ Ab Version 5.0.0 der mGuard-Firmware muss vor der Installation eines Major-Release-Upgrades (z. B. von Version 4.x.y auf 5.x.y oder von Version 5.x.y auf Version 6.x.y) für das betreffende Gerät erst eine Lizenz erworben werden. Die Lizenz muss vor der Durchführung des Firmware-Updates auf dem Gerät installiert werden (siehe „6.2.3 Verwaltung » Lizenzierung“ , „Installieren“ auf Seite 83)
Minor-Release-Upgrades (bedeutet: gleichbleibende Hauptversion, z. B. innerhalb von 5.x.y) können bis auf Weiteres ohne Lizenz installiert werden.

Lokales Update

Dateiname

Zur Installation von Paketen gehen Sie wie folgt vor:

1. Die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und öffnen,

so dass ihr Pfad- bzw. Dateiname im Feld *Dateiname* angezeigt wird.
Das Format des Dateinamens muss lauten: update-a.b.c-d.e.f.default.tar.gz

2. Dann die Schaltfläche **Installiere Pakete** klicken.

Online Update

Um ein Online Update durchzuführen, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass unter **Update Server** mindestens ein gültiger Eintrag vorhanden ist. Die dafür nötigen Angaben haben Sie von Ihrem Lizenzgeber erhalten.
2. Geben Sie den Namen des Package-Sets ein. z.B. „update-4.0.x-4.1.0“.
3. Dann die Schaltfläche **Installiere Package Set** klicken.

Automatische Updates

Dieses ist eine Variante des Online Updates, bei welcher der mGuard das benötigte Package-Set eigenständig ermittelt.

Neuestes Patch-Release installieren (x.y.Z)

Patch-Releases beheben Fehler der vorherigen Versionen und haben eine Versionsnummer, welche sich nur in der dritten Stelle ändern.

Z.B. ist 4.0.1 ein Patch-Release zur Version 4.0.0.

Aktuelles Minor-Release zur Hauptversion installieren (x.Y.z)
Nächstes Major-Release installieren (X.y.z)

Minor- und Major-Releases ergänzen den mGuard um neue Eigenschaften oder enthalten Änderungen am Verhalten des mGuard. Ihre Versionsnummer ändert sich in der ersten oder zweiten Stelle.

Z.B. ist 4.1.0 ein Major- bzw. Minor-Release zu den Versionen 3.1.0 bzw. 4.0.1.

Update Server

Legen Sie fest, von welchen Servern ein Update vorgenommen werden darf.

- Die Liste der Server wird von oben nach unten abgearbeitet, bis ein verfügbarer Server gefunden wird. Die Reihenfolge der Einträge legt also deren Priorität fest.
- Alle konfigurierten Update Server müssen die selben Updates zur Verfügung stellen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Das Update der kann entweder per HTTPS oder HTTP erfolgen.

Server Adresse

Hostnamen des Servers, der die Update-Dateien bereitstellt.

Login

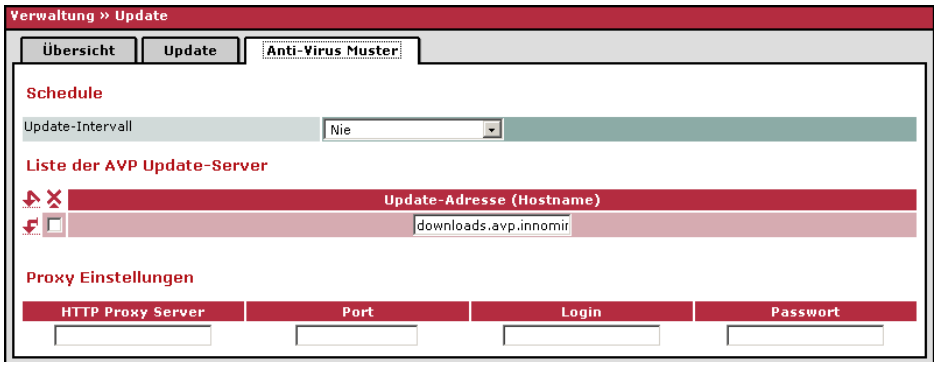
Login für den Server.

Passwort

Passwort für den Login.

Anti-Virus Muster

(Wird nur angezeigt, wenn ein Virenfilter installiert und lizenziert ist.)



Die Dateien mit den Virensignaturen (auch *Anti-Virus Pattern, Anti-Virus-Muster* oder *Virenerkennungs-Muster* genannt) können durch einen einstellbaren Update-Server in einem nutzerdefinierten Intervall aktualisiert werden. Das Update geschieht parallel zur Nutzung des Anti-Virus-Filters. Im Auslieferungszustand befinden sich keine Virensignaturen auf dem mGuard. Deshalb sollte nach dem Aktivieren des Anti-Virus-Schutzes mit der entsprechenden Lizenz auch das Update-Intervall eingestellt werden. Der Verlauf des Updates kann im Anti-Virus-Update-Log verfolgt werden.

Schedule

Update-Intervall

Geben Sie hier an, ob - und wenn ja - in welchen Zeitabständen ein automatisches Update der Virenerkennungs-Muster stattfinden soll. Öffnen Sie dazu die Auswahlliste und wählen Sie den gewünschten Wert.

Die Gesamtgröße der Datenbank beträgt mehrere MByte. Es werden nur die auf dem Update-Server aktualisierten Dateien nachgeladen.

Liste der AVP Update-Server

Geben Sie hier den Namen von mindestes einem AVP Update-Server an.

Sie können die Server auswählen, von denen der Update der Virensignaturdatei geladen werden soll. Ein Standardserver ist bereits voreingetragen. Sie können bei Bedarf eigene Server angeben.

⌦ Die Liste der Server wird von oben nach unten abgearbeitet, bis ein verfügbarer Server gefunden wird. Die Reihenfolge der Einträge legt also deren Priorität fest.

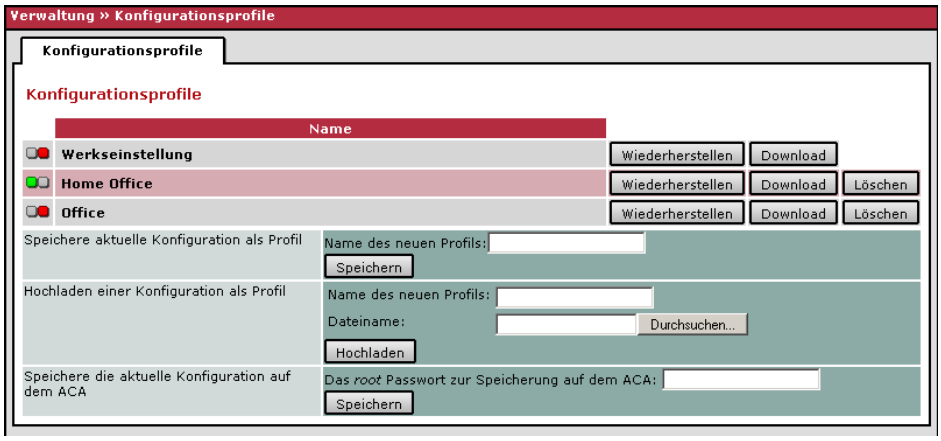
Proxy-Einstellungen

HTTP Proxy Server

Bei Verwendung eines HTTP Proxy Servers geben Sie hier dessen IP-Adresse an sowie die Portnummer des von ihm benutzen **Ports**. Ferner unter **Login** und **Passwort** die Zugangsdaten Benutzername bzw. Passwort.

6.2.5 Verwaltung » Konfigurationsprofile

Konfigurations-profile



Sie haben die Möglichkeit, die Einstellungen des mGuard als Konfigurationsprofil unter einem beliebigen Namen im mGuard zu speichern. Sie können mehrere solcher Konfigurationsprofile anlegen, so dass Sie nach Bedarf zwischen verschiedenen Profilen wechseln können, z. B. wenn der mGuard in unterschiedlichen Umgebungen eingesetzt wird.

Darüber hinaus können Sie Konfigurationsprofile als Dateien auf ihrem Konfigurationsrechner abspeichern. Umgekehrt besteht die Möglichkeit, eine so erzeugte Konfigurationsdatei in den mGuard zu laden und zu aktivieren.

Zusätzlich haben Sie die Möglichkeit, jederzeit die *Werkseinstellung* (wieder) in Kraft zu setzen.

Konfigurationsprofile können beim EAGLE mGuard auch auf einem externen Autokonfigurations-Adapter (ACA) abgelegt werden, der an die V.24/USB Buchse des mGuards angeschlossen werden kann - siehe „Profile auf dem ACA (nur EAGLE mGuard)“ auf Seite 90.

- Beim Abspeichern eines Konfigurationsprofils werden die Passwörter, die zur Authentisierung des administrativen Zugriffs auf den mGuard dienen, nicht mitgespeichert.
- Es ist möglich, ein Konfigurationsprofil zu laden und in Kraft zu setzen, das unter einer älternen Firmware-Version des mGuard erstellt wurde. Umgekehrt trifft das nicht zu: Ein unter einer neueren Firmware-Version erstelltes Konfigurationsprofil sollte nicht geladen werden.

Konfigurationsprofile

Die Seite *Konfigurationsprofile* zeigt oben eine Liste von Konfigurationsprofilen, die im mGuard gespeichert sind, z. B. das Konfigurationsprofil *Werkseinstellung*. Sofern vom Benutzer Konfigurationsprofile gespeichert worden sind (siehe unten), werden diese hier aufgeführt.

Aktives Konfigurationsprofil: Das Konfigurationsprofil, das zurzeit in Kraft ist, hat vorne im Eintrag das *Active*-Symbol - siehe rechts.

Sie können Konfigurationsprofile, die im mGuard gespeichert sind,

- in Kraft setzen
- als Datei auf dem angeschlossenen Konfigurations-Rechner speichern
- löschen
- anzeigen.

Konfigurationsprofil anzeigen:

In der Liste den Namen des Konfigurationsprofils anklicken.

Die Werkseinstellung oder ein vom Benutzer im mGuard gespeichertes Konfigurationsprofil in Kraft setzen

Rechts neben dem Namen des betreffenden Konfigurationsprofils auf die Schaltfläche **Wiederherstellen** klicken.
Folge:

Das betreffende Konfigurationsprofil wird aktiviert.

⌦ Wenn das Wiederherstellen einen Wechsel zwischen dem Stealth-Modus und einem der anderen Netzwerk-Modi beinhaltet, wird der mGuard neu gestartet.

Konfigurationsprofil als Datei auf dem Konfigurations-Rechner speichern

1. Rechts neben dem Namen des betreffenden Konfigurationsprofils auf die Schaltfläche **Download** klicken.
2. Legen Sie im angezeigten Dialogfeld den Dateinamen und Ordner fest, unter bzw. in dem das Konfigurationsprofil als Datei gespeichert werden soll. (Sie können die Datei beliebig benennen.)

Konfigurationsprofil löschen:

Rechts neben dem Namen des betreffenden Konfigurationsprofils auf die Schaltfläche **Löschen** klicken.

⌦ Das Profil **Werkseinstellung** kann nicht gelöscht werden.

Aktuelle Konfiguration als Konfigurationsprofil im mGuard speichern

1. Hinter „Speichere aktuelle Konfiguration als Profil“ in das Feld *Name des neuen Profils* den gewünschten Profil-Namen eintragen.
2. Auf die Schaltfläche **Speichern** klicken.

Folge:
Das Konfigurationsprofil wird im mGuard gespeichert, und der Name des Profils wird in der Liste der bereits im mGuard gespeicherten Profile angezeigt.

Hochladen eines Konfigurationsprofils, das auf dem Konfigurations-Rechner in einer Datei gespeichert ist

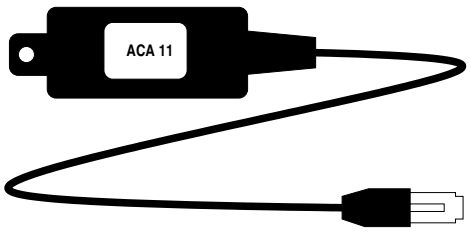
Voraussetzung: Sie haben nach dem oben beschriebenem Verfahren ein Konfigurationsprofil als Datei auf dem Konfigurations-Rechners gespeichert.

1. Hinter „Hochladen einer Konfiguration als Profil“ in das Feld *Name des neuen Profils* den gewünschten Profil-Namen eintragen.
2. Auf die Schaltfläche **Durchsuchen...** klicken und im angezeigten Dialogfeld die betreffende Datei selektieren und öffnen.
3. Auf die Schaltfläche **Hochladen** klicken.

Folge:
Das Konfigurationsprofil wird in den mGuard geladen, und der in Schritt 1 vergebene Name wird in der Liste der bereits im mGuard gespeicherten Profile angezeigt.

Profile auf dem ACA (nur EAGLE mGuard)

Konfigurationsprofile können auch auf einem externen Autokonfigurations-Adapter (ACA) abgelegt werden. Dazu den ACA an die V.24 Buchse (ACA11) oder USB-Buchse (ACA21) des EAGLE mGuard anschließen.



Profil auf dem ACA speichern

1. Wenn das Root-Passwort auf dem EAGLE mGuard, auf welchem das Profil später wieder eingelesen werden soll, ungleich „root“ ist, dann muss dieses Passwort in das Feld **Das root Passwort zur Speicherung auf dem ACA** eingegeben werden.
2. Auf die Schaltfläche **Speichern** klicken.
   Folge:

   Die LED STATUS blinkt (beim ACA11 auch die LED V.24), bis das Speichern beendet ist.

Profil vom ACA laden

Den ACA in die V.24 Buchse des EAGLE mGuard einstecken. Bei eingesecktem ACA den EAGLE mGuard starten. Das Root-Passwort des mGuards muss entweder „root“ lauten oder dem während des Speicherns des Profils angegebenen Passwort entsprechen.

Die LED STATUS blinkt (beim ACA11 auch die LED V.24), bis das Laden beendet ist.

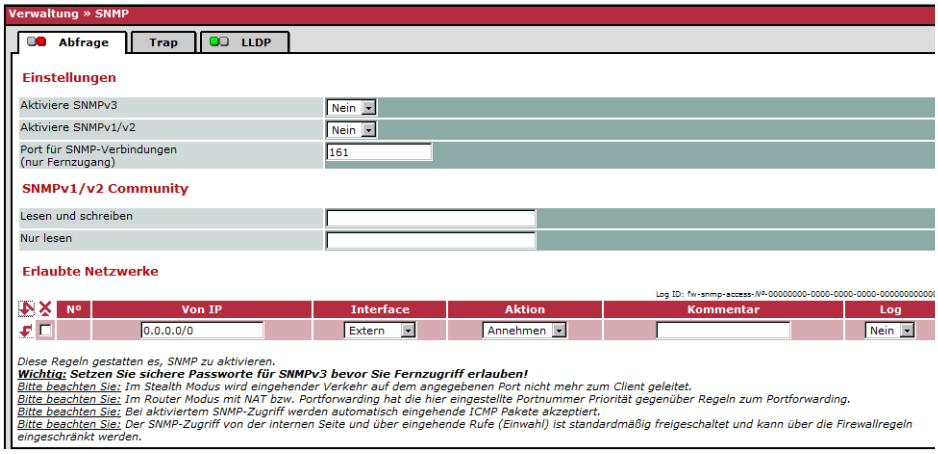
Folge:

Das vom ACA geladene Konfigurationsprofil wird in den EAGLE mGuard geladen und in Kraft gesetzt. Es erscheint nicht in der Liste der im EAGLE mGuard gespeicherten Konfigurationsprofile.

⌧ Die Konfiguration auf dem ACA enthält auch die Passwörter für die Benutzer *root*, *admin*, *netadmin*, *audit* und *user*. Diese werden beim Laden vom ACA ebenfalls übernommen.

6.2.6 Verwaltung » SNMP

Abfrage


Verwaltung » SNMP
Abfrage
Trap
LLDP
Einstellungen
Aktiviere SNMPv3
Nein
Aktiviere SNMPv1/v2
Nein
Port für SNMP-Verbindungen (nur Fernzugang)
161
SNMPv1/v2 Community
Lesen und schreiben
Nur lesen
Erlaubte Netzwerke
Nº
Von IP
Interface
Aktion
Kommentar
Log
0.0.0.0/0
Extern
Annehmen
Nein
Diese Regeln gestatten es, SNMP zu aktivieren.
Wichtig: Setzen Sie sichere Passworte für SNMPv3 bevor Sie Fernzugriff erlauben!
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Bei aktiviertem SNMP-Zugriff werden automatisch eingehende ICMP Pakete akzeptiert.
Bitte beachten Sie: Der SNMP-Zugriff von der internen Seite und über eingehende Rufe (Einwahl) ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Das SNMP (Simple Network Management Protocol) wird vorzugsweise in komplexeren Netzwerken benutzt, um den Zustand und den Betrieb von Geräten zu überwachen.

Das SNMP gibt es in mehreren Entwicklungsstufen: SNMPv1/SNMPv2 und SNMPv3.

Die älteren Versionen SNMPv1/SNMPv2 benutzen keine Verschlüsselung und gelten als nicht sicher. Daher ist davon abzuraten, SNMPv1/SNMPv2 zu benutzen.

SNMPv3 ist unter dem Sicherheitsaspekt deutlich besser, wird aber noch nicht von allen Management-Konsolen unterstützt.

Ist SNMPv3 oder SNMPv1/v2 aktiviert, wird das oben auf der Registerkartenzunge durch ein grünes Signalfeld angezeigt. Sonst, d. h. bei nicht aktivem SNMPv3 und SNMPv1/v2 ist das Signalfeld auf Rot.

⌦ SNMP-„Get“- oder „Walk“-Anfragen können länger als eine Sekunde dauern. Dieser Wert entspricht jedoch dem Standard-Timeout-Wert einiger SNMP-Management-Applikationen.
Bitte setzen Sie aus diesem Grund den Timeout-Wert Ihrer Management Applikation auf Werte zwischen 3 und 5 Sekunden, falls Timeout-Probleme auftreten sollten.

Einstellungen

Aktiviere SNMPv3: Ja / Nein

Wollen Sie zulassen, dass der mGuard per SNMPv3 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.

☞ Um Zugriffs- bzw. Überwachungsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren.

Für den Zugang per SNMPv3 ist eine Authentifizierung mittels Login und Passwort notwendig. Die Werkseinstellungen für die Login-Parameter lauten:

Login: admin

Passwort: SnmpAdmin (Bitte beachten Sie die Groß-/Kleinschreibung!)

Für die Authentifizierung wird MD5 unterstützt, für die Verschlüsselung DES.

Die Login-Parameter für SNMPv3 können nur mittels SNMPv3 geändert werden.

Aktiviere SNMPv1/v2: Ja / Nein

Wollen Sie zulassen, dass der mGuard per SNMPv1/v2 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.
Zusätzlich müssen Sie unter **SNMPv1/v2 Community** die Login-Daten angeben.

☞ Um Zugriffs- bzw. Überwachungsmöglichkeiten auf den mGuard differenziert festzulegen, müssen Sie auf dieser Seite unter **Erlaubte Netzwerke** die Firewall-Regeln für die verfügbaren Interfaces entsprechend definieren.

Port für SNMP-Verbindungen

Standard: 161

Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2, VPN* und *Einwahl*. Für internen Zugriff gilt weiterhin 161.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe gegebenenfalls die Port-Nummer angeben, die hier festgelegt ist.

SNMPv1/v2 Community

Lesen und schreiben

Nur lesen

Geben Sie in diese Felder die erforderlichen Login-Daten ein.

Erlaubte Netzwerke

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SNMP-Zugriffs.

Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere SNMPv3** oder **Aktiviere SNMPv1/v2** auf **Ja** steht.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt beziehungsweise verboten ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- Eine IP Addresse.
- Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.
- **0.0.0.0/0** bedeutet alle Adressen.

Interface

Extern / Intern / Extern 2 / VPN / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

1. *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

Sind keine Regeln gesetzt oder greift keine Regel, gelten folgende Standardeinstellungen:

SNMP-Überwachung ist erlaubt über *Intern, VPN* und *Einwahl*.
Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Überwachungsmöglichkeiten nach Bedarf fest.

Vorsicht:

Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewallregeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen. Damit Sie sich nicht aussperren, müssen Sie eventuell gleichzeitig den Zugriff über ein anderes Interface explizit mit *Annehmen* erlauben, bevor Sie durch Klicken auf die **Übernehmen**-Schaltfläche die neue Einstellung in Kraft setzen. Sonst muss bei Aussperrung die Revovery-Prozedur durchgeführt werden.

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

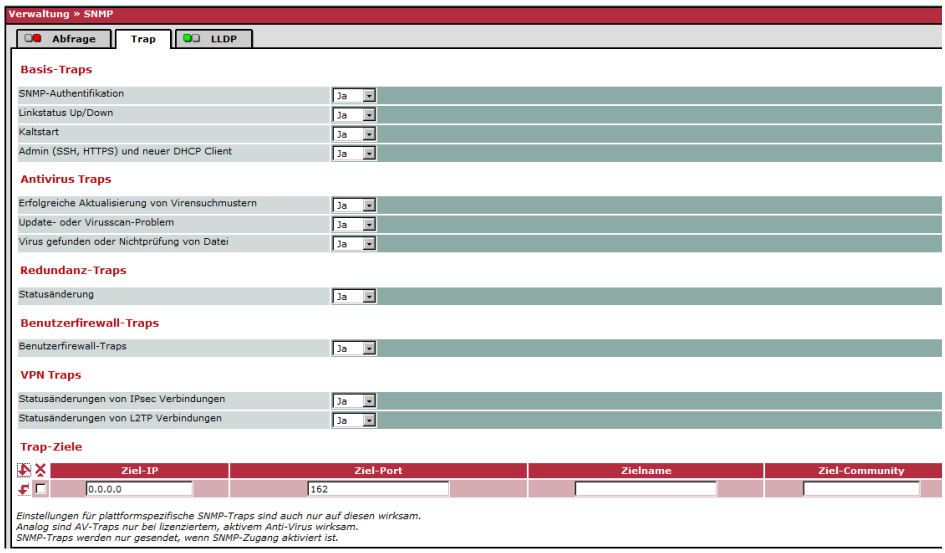
Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Trap



Bei bestimmten Ereignissen kann der mGuard SNMP Traps (→ Glossar) versenden. Die Traps entsprechen SNMPv1. Im Folgenden sind die zu jeder Einstellung zugehörigen Trap-Informationen aufgelistet, deren genaue Beschreibung in der zum mGuard gehörenden MIB zu finden ist.

⌦ Werden SNMP Traps über einen VPN-Kanal zur Gegenstelle gesendet, dann muss sich die IP-Adresse der Gegenstelle in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote**-Netzwerk angegeben ist. Und die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Lokal** angegeben ist (siehe „VPN-Verbindung / VPN-Verbindungskanäle definieren“ auf Seite 214).

– Ist dabei die Option **Aktiviere 1-zu-1-NAT des lokalen Netzwerkes in ein internes Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 220), gilt Folgendes: Die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das mit **Interne Netzwerkadresse für lokales 1-zu-1-NAT** angegeben ist.

– Ist dabei die Option **Aktiviere 1-zu-1-NAT des gegenüberliegenden Netzwerkes auf ein anders Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 220), gilt Folgendes: Die IP-Adresse des Trap-Empfängers muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote** angegeben ist.

Basis-Traps

- **SNMP-Authentifikation**: Traps aktivieren **Ja / Nein**
  enterprise-oid : mGuardInfo
  generic-trap : authenticationFailure
  specific-trap : 0
  Erläuterung : Wird gesendet, falls eine Station versucht, unberechtigt auf den SNMP Agenten des mGuard zuzugreifen.

- **Linkstatus Up/Down**: Traps aktivieren **Ja / Nein**
  enterprise-oid : mGuardInfo
  generic-trap : linkUp, linkDown
  specific-trap : 0

Erläuterung : Wird gesendet, wenn die Verbindung zu einem Port unterbrochen (linkDown) bzw. wiederhergestellt (linkUp) wird.

- **Kaltstart**: Traps aktivieren **Ja / Nein**
  enterprise-oid : mGuardInfo
  generic-trap : coldStart
  specific-trap : 0
  Erläuterung : Wird nach Kalt- oder Warmstart gesendet.

- **Admin (SSH, HTTPS) Traps und neuer DHCP Client**: Traps aktivieren **Ja / Nein**
  enterprise-oid : mGuardb
  generic-trap : enterpriseSpecific
  specific-trap : mGuardHTTPSLoginTrap (1)
  additional : mGuardHTTPSLastAccessIP
  Erläuterung : Dieser Trap wird gesendet, wenn jemand versucht, eine HTTPS-Sitzung mit einem falschen Passwort zu öffnen. Der Trap enthält die IP-Adresse des letzten fehlgeschlagenen Versuchs der Login-Anfrage.

  enterprise-oid : mGuard
  generic-trap : enterpriseSpecific
  specific-trap : mGuardShellLoginTrap (2)
  additional : mGuardShellLastAccessIP
  Erläuterung : Dieser Trap wird gesendet, wenn jemand die Shell öffnet per SSH oder über die serielle Schnittstelle. Der Trap enthält die IP-Adresse der Login-Anfrage. Wurde diese Anfrage über die serielle Schnittstelle abgesetzt, lautet der Wert von 0.0.0.0.

  enterprise-oid : mGuard
  generic-trap : enterpriseSpecific
  specific-trap : 3
  additional : mGuardHTTPSLastAccessMAC
  Erläuterung : Dieser Trap wird gesendet, wenn eine DHCP-Anfrage von einem unbekannten Client eingegangen ist.

Hardwarebezogene Traps (nur mGuard industrial RS und EAGLE mGuard)

- **Chassis (Stromversorgung, Relais)**: Traps aktivieren **Ja / Nein**
  enterprise-oid : mGuardTrapSenderIndustrial
  genericTrap : enterpriseSpecific
  specific-trap : mGuardTrapIndustrialPowerStatus (2)
  additional : mGuardTrapIndustrialPowerStatus
  Erläuterung : Wird gesendet, wenn das System einen Stromausfall registriert.

  enterprise-oid : mGuardTrapSenderIndustrial
  genericTrap : enterpriseSpecific
  specific-trap : mGuardTrapSignalRelais (3)
  additional : mGuardTResSignalRelaisState

(mGuardTEsSignlalRelaisReason, mGuardTResSignal RelaisReasonIdx)

Erläuterung : Wird gesendet nach geändertem Meldekontakt und gibt den dann aktuellen Status an (0 = Aus, 1 = Ein).

- **Agent (ACA, Temperatur):** Traps aktivieren **Ja / Nein**

enterprise-oid : mGuardTrapIndustrial
genericTrap : enterpriseSpecific
specific-trap : mGuardTrapIndustrialTemperature (1)
additional : mGuardSystemTemperature, mGuardTrapIndustrialTempHiLimit, mGuardTrapIndustrialLowLimit
Erläuterung : Bei Überschreitung der festgelegten Grenzwerte gibt der Trap die Temperatur an.

enterprise-oid : mGuardTrapIndustrial
genericTrap : enterpriseSpecific
specific-trap : mGuardTrapAutoConfigAdapterState (4)
additional : mGuardTrapAutoConfigAdapterChange
Erläuterung : Dieser Trap wird nach Zugriff auf den ACA gesendet.

Blade Kontroller Traps (nur blade)

- **Statusänderung von Blades** (Umstecken, Ausfall): Traps aktivieren **Ja / Nein**

enterprise-oid : mGuardTrapBladeCTRL
generic-trap : enterpriseSpecific
specific-trap : mGuardTrapBladeCtrlPowerStatus (2)
additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlPowerStatus
Erläuterung : Trap wird gesendet, wenn der Stromversogungsstatus des Blade Pack wechselt.

enterprise-oid : mGuardTrapBladeCTRL
generic-trap : enterpriseSpecific
specific-trap : mGuardTrapBladeCtrlRunStatus (3)
additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlRunStatus
Erläuterung : Trap wird gesendet, wenn der Blade-Ausführungsstatus wechselt.

- **Rekonfiguration von Blades** (Backup/Restore): Traps aktivieren **Ja / Nein**

enterprise-oid : mGuardTrapBladeCtrlCfg
generic-trap : enterpriseSpecific
specific-trap : mGuardTrapBladeCtrlCfgBackup (1)
additional : mGuardTrapBladeRackID, mGuardTrapBladeSlotNr, mGuardTrapBladeCtrlCfgBakkup
Erläuterung : Trap bei Auslösung des Konfigurations-Backups zum Blade-Kontroller.

enterprise-oid : mGuardTrapBladeCtrlCfg
generic-trap : enterpriseSpecific
specific-trap : mGuardTrapBladeCtrlCfgRestored 2
additional : mGuardTrapBladeRackID,
mGuardTrapBladeSlotNr,
mGuardTrapBladeCtrlCfgRestored
Erläuterung : Trap bei Auslösung der Konfigurations-Wiederherstellung vom Blade-Kontroller.

Anti-Virus Traps

- **Erfolgreiche Aktualisierung von Virensuchmustern**: Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : mGuardTrapAvUpdateDone (1)
  additional : mGuardTResAvUpdateDone
  Erläuterung : Trap nach erfolgreichem AV-Update.

- **Update- oder Virusscan-Problem**: Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : mGuardTrapAvUpdateError (2)
  additional : mGuardTResAvUpdateError
  Erläuterung : Trap bei Fehler während der Durchführung des AV-Updates.

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : mGuardTrapAvFailed (5)
  additional : mGuardTResAvFailed
  Erläuterung : Trap bei allgemeinem AV-Fehler.

- **Virus gefunden oder Nichtprüfung von Datei**: Traps aktivieren **Ja / Nein**

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : mGuardTrapAvVirusDetected (3)
  additional : mGuardTResAvVirusDetected
  Erläuterung : Trap bei Auffinden eines Virus durch die AV-Funktion.

  enterprise-oid : mGuardTrapAv
  generic-trap : enterpriseSpecific
  specific-trap : mGuardTrapAvFileNotScanned (4)
  additional : mGuardTResAvFileNotScanned
  Erläuterung : Trap, wenn die Datei nicht nach Viren gescannt worden ist.

Redundanz Traps

- **Statusänderung**: Traps aktivieren **Ja / Nein**.

  enterprise-oid : mGuardTrapRouterRedundancy
  genericTrap : enterpriseSpecific
  specific-trap : mGuardTrapRouterRedStatusChange TRAP-TYPE (1)
  additional : mGuardTResRedundancyState,

mGuardTResRedundancyReason
Erläuterung : Trap nach Wechsel des aktuellen HA-Cluster-Status.

enterprise-oid : mGuardTrapRouterRedundancy
genericTrap : enterpriseSpecific
specific-trap : mGuardTrapRouterRedBackupDown TRAP-TYPE (2)
additional : mGuardTResRedundancyBackupDown
Erläuterung : Trap wird gesendet, wenn das Master-Gerät das Backup-Gerät nicht erreichen kann. (Wird nur gesendet, wenn ICMP-Prüfungen aktiviert sind.)

Benutzerfirewall-Traps: Ja / Nein

enterprise-oid : mGuardTrapUserFirewall
generic-trap : enterpriseSpecific
specific-trap : mGuardTrapUserFirewallLogin (1)
additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod
Erläuterung : Trap bei Einloggen eines Benutzers der Benutzer-Firewall.

enterprise-oid : mGuardTrapUserFirewall
generic-trap : enterpriseSpecific
specific-trap : mGuardTrapUserFirewallLogout (2)
additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallLogoutReason
Erläuterung : Trap bei Ausloggen eines Benutzers der Benutzer-Firewall.

enterprise-oid : mGuardTrapUserFirewall
generic-trap : enterpriseSpecific
specific-trap : mGuardTrapUserFirewallAuthError TRAP-TYPE (3)
additional : mGuardTResUserFirewallUsername, mGuardTResUserFirewallSrcIP, mGuardTResUserFirewallAuthenticationMethod
Erläuterung : Trap bei Authentifizierungs-Fehler.

VPN Traps

- **Statusänderungen von IPsec Verbindungen**: **Ja / Nein**.

enterprise-oid : mGuardTrapVPN
genericTrap :enterpriseSpecific
specific-trap :mGuardTrapVPNIKEServerStatus (1)
additional :mGuardTResVPNStatus
Erläuterung : Trap beim Starten und Stoppen des IPsec IKE Servers

enterprise-oid :mGuardTrapVPN
genericTrap :enterpriseSpecific
specific-trap :mGuardTrapVPNIPsecConnStatus (2)
additional :mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuardTResVPNType, mGuardTResVPNLocal, mGuardTResVPNRemote
Erläuterung :Trap bei Zustandsänderung einer IPsec Verbindung

- **Statusänderungen von L2TP Verbindungen**: **Ja / Nein**.
  enterprise-oid :mGuardTrapVPN
  genericTrap :enterpriseSpecific
  specific-trap :mGuardTrapVPNL2TPConnStatus (3)
  additional :mGuardTResVPNName, mGuardTResVPNIndex, mGuardTResVPNPeer, mGuardTResVPNStatus, mGuard-TResVPNLocal, mGuardTResVPNRemote
  Erläuterung :Trap bei Zustandsänderung einer L2TP Verbindung

SNMP Trap-Ziele

Traps können an mehrere Ziele versendet werden.

Ziel-IP

IP-Adresse, an welche der Trap gesendet werden soll.

Ziel-Port

Standard: 162

Ziel-Port, an welchen der Trap gesendet werden soll

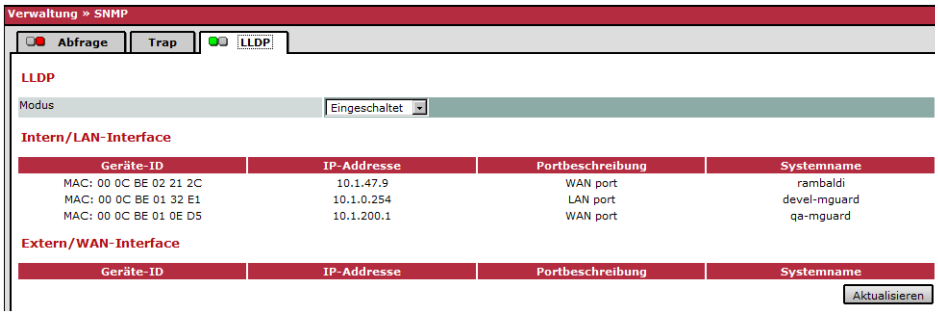
Zielname

Ein optionaler beschreibender Name für das Ziel. Hat keinen Einfluss auf die generierten Traps.

Ziel-Community

Name der SNMP-Community, welcher der Trap zugeordnet ist.

LLDP



Mit LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) kann mit geeigneten Abfragemethoden die (Ethernet) Netzwerk-Infrastruktur automatisch ermittelt werden. Auf Ethernet-Ebene (Layer 2) werden dazu periodisch Multicasts versandt. Aus deren Antworten werden dann Tabellen der ans Netz angeschlossenen Systeme erstellt, die über SNMP abgefragt werden können.

LLDP

Modus: Eingeschaltet / Ausgeschaltet

Der LLDP-Service bzw. -Agent kann hier global ein- bzw. ausgeschaltet werden. Ist die Funktion eingeschaltet, wird das oben auf der Registerkartenzunge durch ein grünes Signalfeld angezeigt. Ist das Signalfeld auf Rot, ist die Funktion ausgeschaltet.

Intern/LAN-Interface

und

Extern/WAN-Interface

Geräte-ID

Eine eindeutige ID des gefundenen Rechners; üblicherweise eine seiner MAC-Adressen.

IP-Adresse

IP-Adresse des gefundenen Rechners über die der Rechner per SNMP administriert werden kann.

Portbeschreibung

Ein Text, welcher die Netzwerkschnittstelle beschreibt, über welche der Rechner gefunden wurde.

Systemname

Hostname des gefundenen Rechners.

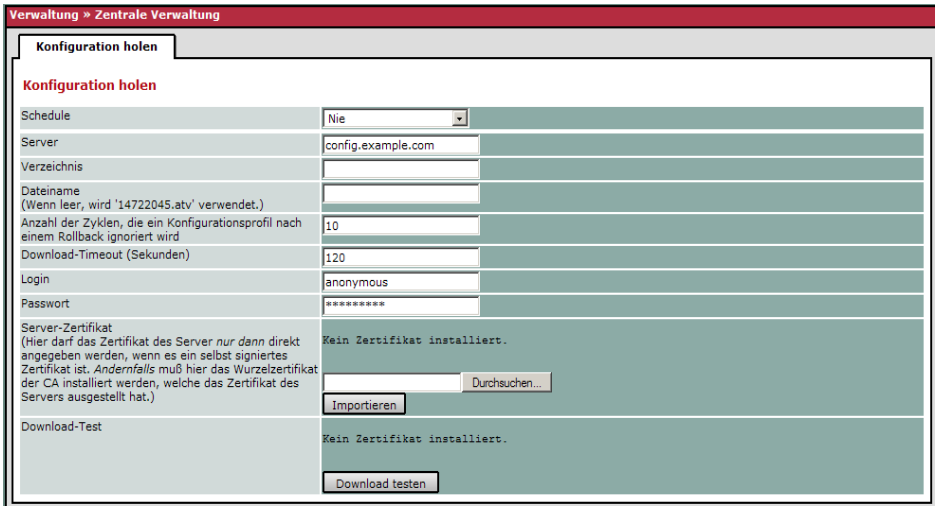
Schaltflächen

Aktualisieren

Um gegebenenfalls die angezeigten Daten auf den aktuellen Stand zu bringen, auf die Schaltfläche **Aktualisieren** klicken.

6.2.7 Verwaltung » Zentrale Verwaltung

Konfiguration holen



Der mGuard kann sich in einstellbaren Zeitintervallen neue Konfigurationsprofile von einem HTTPS Server holen, wenn der Server sie dem mGuard als Datei zur Verfügung stellt (Datei-Endung: .atv). Wenn sich die jeweils zur Verfügung gestellte Konfiguration von der aktuellen Konfiguration des mGuard unterscheidet, wird die verfügbare Konfiguration automatisch heruntergeladen und aktiviert.

Konfiguration holen

Schedule

Geben Sie hier an, ob - und wenn ja - wann bzw. in welchen Zeitabständen der mGuard versuchen soll, eine neue Konfiguration vom Server herunterzuladen und bei sich in Kraft zu setzen. Öffnen Sie dazu die Auswahlliste und wählen Sie den gewünschten Wert.

Bei Auswahl von **Zeitgesteuert** wird unterhalb ein neues Feld eingeblendet. In diesem geben Sie an, ob täglich oder an einem bestimmten Wochentag regelmäßig und zu welcher Uhrzeit eine neue Konfiguration vom Server heruntergeladen werden soll.

Das zeitgesteuerte Herunterladen einer neuen Konfiguration kann erst nach Synchronisation der Systemzeit erfolgen - siehe „Verwaltung » Systemeinstellungen“, „Zeit und Datum“ auf Seite 63.

Die Zeitsteuerung setzt die ausgewählte Zeit in Bezug auf die eventuell konfigurierte Zeitzone.

Server

IP-Adresse oder Hostname des Servers, welcher die Konfigurationen bereitstellt.

Verzeichnis

Das Verzeichnis (Ordner) auf dem Server, in dem die Konfiguration liegt.

Dateiname

Der Name der Datei in dem oben definierten Verzeichnis. Falls an dieser Stelle kein Dateiname definiert ist, wird die Seriennummer des mGuards inklusive der Endung „.atv“ verwendet.

Anzahl der Zyklen, die ein Konfigurationsprofil nach einem Rollback ignoriert wird

Standard: 10

Nach Holen einer neuen Konfiguration könnte es im Prinzip passieren, dass nach Inkraftsetzen der neuen Konfiguration der mGuard nicht mehr erreichbar ist und damit eine neue, korrigierende Fernkonfiguration nicht mehr möglich ist. Um das auszuschließen, unternimmt der mGuard folgende Prüfung:

Sofort nach Inkraftsetzen der geholten Konfiguration versucht der mGuard auf Grundlage dieser neuen Konfiguration, die Verbindung zum Konfigurations-Server nochmals herzustellen und das neue, bereits in Kraft gesetzte Konfigurationsprofil erneut herunterzuladen.

Wenn das gelingt, bleibt die neue Konfiguration in Kraft.

Wenn diese Prüfung negativ ausfällt - aus welchen Gründen auch immer -, geht der mGuard davon aus, dass das gerade in Kraft gesetzte neue Konfigurationsprofil fehlerhaft ist. Für Identifizierungszwecke merkt sich der mGuard dessen MD5-Summe. Dann führt der mGuard ein Rollback durch. Rollback bedeutet, dass die letzte (funktionierende) Konfiguration wiederhergestellt wird. Das setzt voraus, dass in der neuen (nicht funktionierenden) Konfiguration die Anweisung steht, ein Rollback durchzuführen, wenn ein neues geladenes Konfigurationsprofil sich in dem oben beschriebenen Prüfungsverfahren als fehlerhaft erweist.

Wenn nach der im Feld **Schedule** (und **Zeitgesteuert**) festgelegten Zeit der mGuard erneut und zyklisch versucht, ein neues Konfigurationsprofil zu holen, wird er ein solches nur unter folgendem Auswahlkriterium annehmen: Das zur Verfügung gestellte Konfigurationsprofil muss sich unterscheiden von dem Konfigurationsprofil, das sich für den mGuard zuvor als fehlerhaft erwiesen hat und zum Rollback geführt hat. (Dazu vergleicht der mGuard die bei ihm gespeicherte MD5-Summe der alten, für ihn fehlerhaften und verworfenen Konfiguration mit der MD5-Summe des angebotenen neuen Konfigurationsprofils.)

Wird dieses Auswahlkriterium erfüllt, d. h. es wird ein neueres Konfigurationsprofil angeboten, holt sich der mGuard dieses Konfigurationsprofil, setzt es in Kraft und prüft es gemäß des oben beschriebenen Verfahrens - und setzt es bei nicht bestandener Prüfung per Rollback wieder außer Kraft.

Wird dieses Auswahlkriterium nicht erfüllt (weil immer noch das selbe Konfigurationsprofil angeboten wird), bleibt für die weiteren zyklischen Abfragen dieses Auswahlkriterium so lange in Kraft, wie in diesem Feld (**Anzahl der Zyklen...**) festgelegt ist. Ist die hier festgelegte Anzahl von Zyklen abgelaufen, ohne dass das auf dem Konfigurations-Server angebotene Konfigurationsprofil verändert wurde, setzt der mGuard das unveränderte neue ("fehlerhafte") Konfigurationsprofil ein weiteres Mal in Kraft, obwohl es sich als "fehlerhaft" erwiesen hatte. Das geschieht um auszuschließen, dass das Misslingen der Prüfung durch äußere Faktoren (z. B. Netzwerkausfall) bedingt war. Der mGuard versucht dann erneut, auf Grundlage der erneut eingesetzten neuen Konfiguration die Verbindung zum Konfigurations-Server herzustellen und erneut das neue, jetzt in Kraft gesetzte Konfigurationsprofil herunterzuladen. Wenn das misslingt, erfolgt wieder ein Rollback, und für die weiteren Zyklen zum Laden einer neuen Konfiguration wird erneut das Auswahlkriterium in Kraft gesetzt - so oft, wie in diesem Feld (**Anzahl der Zyklen...**) festgelegt ist.

Wird im Feld **Anzahl der Zyklen...** als Wert **0** (Null) festgelegt, hat das zur Folge, dass das Auswahlkriterium - das angebotene Konfigurationsprofil wird ignoriert, wenn es unverändert geblieben ist - niemals in Kraft tritt. Dadurch könnte das 2. der nachfolgend aufgeführten Ziele nicht realisiert werden.

Dieser Mechanismus hat folgende Ziele:

1. Nach Inkraftsetzen einer neuen Konfiguration muss sichergestellt sein, dass der mGuard sich weiterhin vom entfernten Standort aus konfigurieren lässt.
2. Bei eng gesetzten Zyklen (z. B. bei **Schedule** = 15 Minuten) muss verhindert werden, dass der mGuard stur ein möglicherweise fehlerhaftes Konfigurationsprofil in zu kurzen Abständen immer wieder erneut testet. Das könnte dazu führen, dass der mGuard so mit sich selbst beschäftigt ist, dass ein administrativer Eingriff von außen behindert oder verhindert wird.
3. Es muss mit großer Wahrscheinlichkeit ausgeschlossen werden, dass äußere Faktoren (z. B. Netzwerkausfall) den mGuard bewogen haben, eine Neukonfiguration als fehlerhaft zu betrachten.

☞ Von Innominate wird ein Application Note zur Verfügung gestellt. Darin ist beschrieben, wie über ein Konfigurationsprofil ein Rollback angewiesen werden kann.

Download-Timeout (Sekunden)

Standard: 120. Gibt an, wie lange während eines Downloads der Konfigurationsdatei ein Timeout (Zeit der Inaktivität) maximal dauern darf. Bei Überschreitung wird der Download abgebrochen. Ob - und wenn ja - wann ein nächster Download-Versuch stattfindet, richtet sich nach der Einstellung von *Schedule* (s. o.).

Login

Login (Benutzername), den der HTTPS Server abfragt.

Passwort

Passwort, das der HTTPS Server abfragt.

Server-Zertifikat

Das Zertifikat, mit dem der mGuard prüft, dass das vom Konfigurations-Server "vorgezeigte" Zertifikat echt ist. Es verhindert, dass von einem nicht autorisierten Server falsche Konfigurationen auf dem mGuard installiert werden.

Hier darf entweder

– ein selbst signiertes Zertifikat des Konfigurations-Servers angegeben werden (also das Gegenstellenzertifikat des selbst signierten Maschinenzertifikats des Konfigurations-Servers),

ODER

– das Wurzelzertifikat der CA (Certification Authority), welche das Zertifikat des Servers ausgestellt hat. Das gilt dann, wenn es sich beim Zertifikat des Konfigurations-Servers um ein von einer CA signiertes Zertifikat handelt (statt um ein selbst signiertes).

☞ Wenn die hinterlegten Konfigurationsprofile auch den privaten VPN-Schlüssel für die VPN-Verbindung oder VPN-Verbindungen mit PSK

enthalten, sollten folgende Bedingungen erfüllt sein:

- Das Passwort sollte aus mindestens 30 zufälligen Groß- und Kleinbuchstaben sowie Ziffern bestehen, um unerlaubten Zugriff zu verhindern.
- Der HTTPS Server sollte über den angegebenen Login nebst Passwort nur Zugriff auf die Konfiguration dieses einen mGuard ermöglichen. Ansonsten könnten sich die Benutzer anderer mGuards Zugriff verschaffen.

☞ Die unter *Server* angegebene IP-Adresse bzw. der Hostname muss im Server-Zertifikat als Common Name (CN) angegeben sein.

☞ Selbstunterschriebene Zertifikate (self-signed) sollten nicht die „key-usage“ Erweiterung verwenden.

Zum Installieren eines Zertifikats wie folgt vorgehen:

Voraussetzung:
Die Zertifikatsdatei ist auf dem angeschlossenen Rechner gespeichert

1. **Durchsuchen...** klicken, um die Datei zu selektieren.
2. **Importieren** klicken.

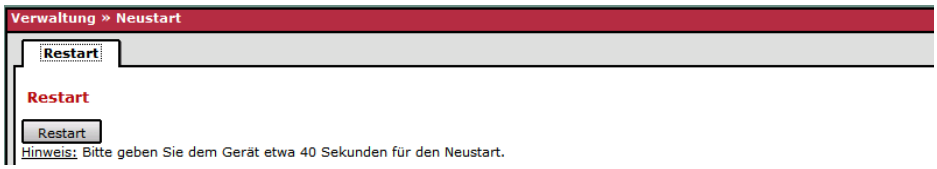
Download-Test

Durch Klicken auf die Schaltfläche **Download testen** können Sie testen – ohne die geänderten Parameter zu speichern oder das Konfigurationsprofil zu aktivieren – ob die angegebenen Parameter funktionieren. Das Ergebnis des Tests wird in der rechten Spalte angezeigt.

⌦ Stellen Sie sicher, dass das Profil auf dem Server keine unerwünschten mit „GAI_PULL_“ beginnenden Variablen enthält, welche die hier vorgenommene Konfiguration überschreiben.

6.2.8 Verwaltung » Neustart

Restart

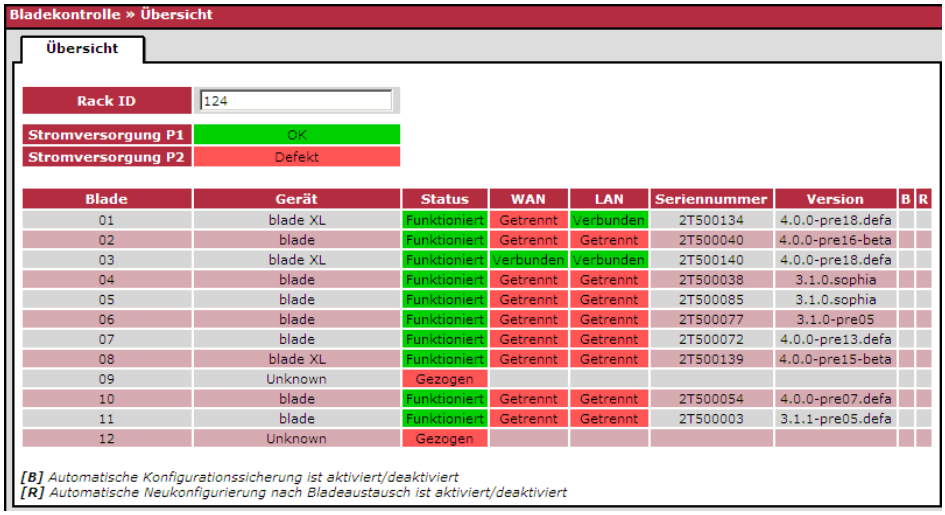


Startet den mGuard neu. Hat den selben Effekt, als wenn Sie die Stromzufuhr vorübergehend unterbrechen, so dass der mGuard aus- und wieder eingeschaltet wird.
Ein Neustart (= Reboot) ist erforderlich im Fehlerfall. Außerdem kann es erforderlich sein nach einem Software-Update.

6.3 Menü Bladekontrolle (nur blade Kontroller)

Dieses Menü steht nur auf dem Kontroller Blade zur Verfügung.

6.3.1 Bladekontrolle » Übersicht



Rack ID

Die ID des Racks, in dem sich der mGuard befindet. Auf dem Kontroller kann dieser Wert für alle blades konfiguriert werden.

Stromversorgung P1/P2

Status der Netzteile P1 und P2.

- OK
- Gezogen
- Defekt
- Fataler Fehler

Blade

Nummer des Slots, in welchem das mGuard blade steckt.

Gerät

Name des Geräts, z.B. „blade“ oder „blade XL“.

Status

Funktioniert - Das Gerät in dem Slot ist funktionsbereit.

Gesteckt - Das Gerät ist vorhanden, aber noch nicht bereit, z. B. weil es gerade beim Starten ist.

Gezogen - In dem Slot wurde kein Gerät entdeckt.

WAN

Status des WAN-Ports.

LAN

Status des LAN-Ports.

Seriennummer

Seriennummer des mGuards.

Version

Softwareversion des mGuards.

B

Backup: Für diesen Slot ist die automatische Konfigurationssicherung auf dem Kontroller aktiviert/deaktiviert.

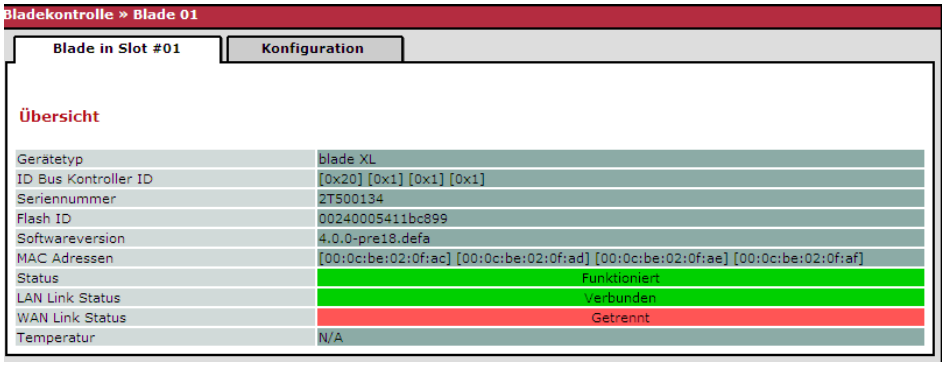
R

Restore: Für diesen Slot ist das automatische Zurückspielen der Konfiguration nach Austausch des mGuards aktiviert/deaktiviert.

6.3.2 Bladekontrolle » Blade 01 bis 12

Diese Seiten zeigen für jeden installierten mGuard Statusinformationen an und erlauben das Speichern und Zurückspielen der Konfiguration des jeweiligen mGuards.

Blade in slot #...



Gerätetyp

Name des Geräts, z.B. „blade“ oder „blade XL“.

ID bus Kontroller ID

ID dieses Slots am Kontrollbus der bladeBase.

Seriennummer

Seriennummer des mGuards.

Flash ID

Flash ID des Flashspeichers des mGuards.

Software Version

Die Version der auf dem mGuard installierten Software.

MAC Adressen

Alle vom mGuard verwendeten MAC-Adressen.

Status

Status des mGuards.

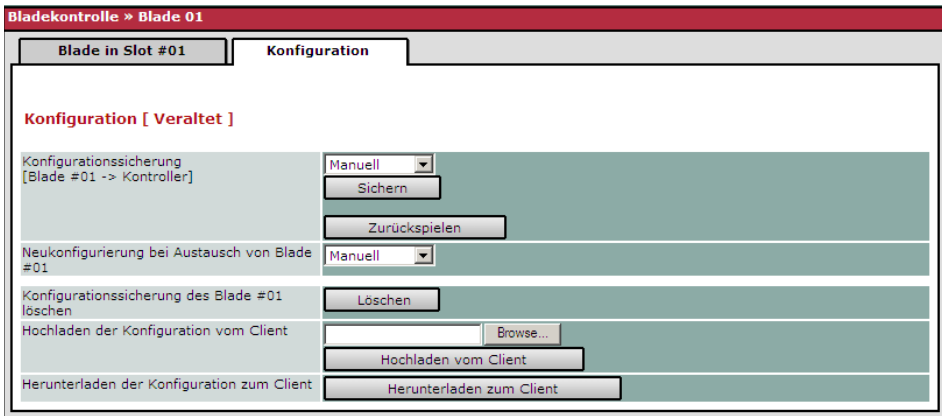
LAN Status

Status des LAN-Ports.

WAN Status

Status des WAN-Ports.

Konfiguration



Konfigurationssicherung [Blade #__ -> Kontroller]

Automatisch: Kurz nach einer Konfigurationsänderung des mGuards wird die neue Konfiguration automatisch auf dem Kontroller gespeichert.

Manuell: Die Konfiguration kann mit **Sichern** auf dem Kontroller gesichert werden.

Mit **Zurückspielen** kann die auf dem Kontroller gesicherte Konfiguration in den mGuard übertragen werden.

☞ Wurde nach einer manuellen Konfigurationssicherung das Blade umkonfiguriert, aber die neue Konfiguration nicht erneut gesichert, ist die im Kontroller gespeicherte Konfiguration veraltet. Dies wird auf der Registerkarte *Konfiguration* durch "Konfiguration [Veraltet]" angezeigt - siehe oben abgebildeter Screenshot.
Das ist als Hinweis auf ein Versäumnis zu verstehen: Sorgen Sie in diesem Fall für die Konfigurationssicherung auf den Kontroller.

Neukonfiguration bei Austausch des Blade

Beim Austausch eines mGuards in diesem Slot wird die auf dem Kontroller gespeicherte Konfiguration auf das neue Gerät in diesem Slot übertragen.

Konfigurationssicherung des Blade #__ löschen

Löscht die auf dem Kontroller gespeicherte Konfiguration für das Gerät in diesem Slot.

Hochladen der Konfiguration vom Client

Hochladen und Speichern des angegebenen Konfigurationsprofils für diesen Slot auf dem Kontroller.

Herunterladen der Konfiguration zum Client

Lädt das auf dem Kontroller gespeicherte Konfigurationsprofil für diesen Slot auf den Konfigurations-PC.

6.4 Menü Netzwerk

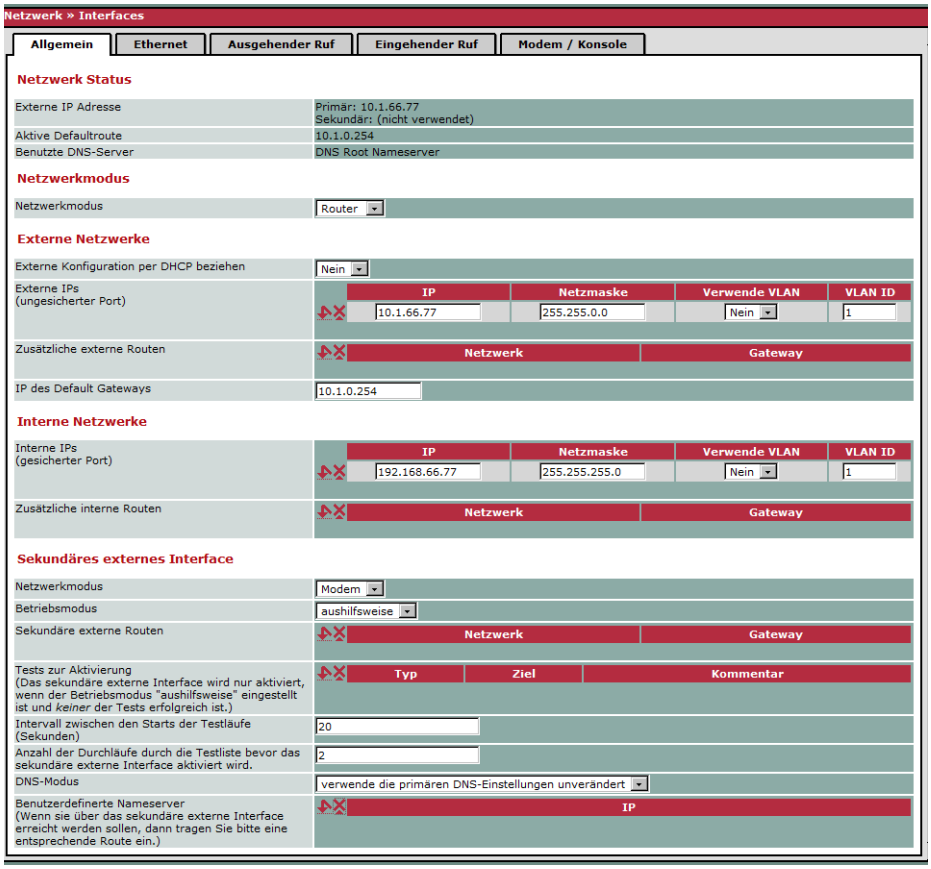
6.4.1 Netzwerk » Interfaces

Der mGuard verfügt über folgende von außen zugängliche Interfaces (Schnittstellen):

	Ethernet: Intern: LAN Extern: WAN	Serielle Schnittstelle	Eingebautes Modem
mGuard Smart	**ja**	**nein**	**nein**
mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta	**ja**	**ja**	**nein**
optional: mGuard industrial RS	**ja**	**ja**	**ja**

Der LAN-Port wird an einen Einzelrechner oder das lokale Netzwerk (= intern) angeschlossen. Der WAN-Port ist für den Anschluss an das externe Netz. Bei Geräten mit serieller Schnittstelle kann der Anschluss ans externe Netz auch oder zusätzlich über die serielle Schnittstelle mittels eines Modems erfolgen. Alternativ kann die serielle Schnittstelle auch wie folgt benutzt werden: für ppp-Einwahl ins lokale Netz oder für Konfigurationszwecke. Bei Geräten mit eingebautem Modem (Analog-Modem oder ISDN-Terminaladapter) kann zusätzlich das Modem benutzt werden, um Zugriffsmöglichkeiten zu kombinieren.

Die Details dazu müssen auf den Registerkarten *Allgemein, Ethernet, Ausgehender Ruf, Eingehender Ruf* und *Modem / Konsole* konfiguriert werden. Für weitere Erläuterungen zur Nutzungsmöglichkeit der seriellen Schnittstelle (und eines eingebauten Modems) siehe „Modem / Konsole“ auf Seite 139.



Allgemein

Netzwerk Status

Externe IP Adresse - Adresse des WAN-Ports

Nur Anzeige: Die Adressen, unter denen der mGuard von Geräten des externen Netzes aus erreichbar ist. Sie bilden die Schnittstelle zu anderen Teilen des LAN oder zum Internet. Findet hier der Übergang zum Internet statt, werden die IP-Adressen normalerweise vom Internet Service Provider (ISP) vorgegeben. Wird dem mGuard eine IP-Adresse dynamisch zugeteilt, können Sie hier die gerade gültige IP-Adresse nachschlagen.

Im *Stealth*-Modus übernimmt der mGuard die Adresse des lokal angeschlossenen Rechners als seine externe IP.

Status des Netzwerk-Modus

Anzeige des Status des ausgewählten Netzwerk Modus.

Aktive Defaultroute

Nur Anzeige: Hier wird die IP-Adresse angezeigt, über die der mGuard versucht, ihm unbekannte Netze zu erreichen. Hier kann insbesondere dann „(none)“ stehen, wenn sich der mGuard im *Stealth*-Modus befindet.

Benutzte DNS-Server

Nur Anzeige: Hier wird der Name der DNS Server angezeigt, die vom mGuard zur Namensauflösung benutzt werden. Diese Information kann nützlich sein, wenn der mGuard z. B. die DNS-Server verwendet, welche ihm vom Internet Service Provider vorgegeben werden.

Netzwerk-Modus: Stealth / Router / PPPoE / PPTP / Modem* / Eingebautes Modem*

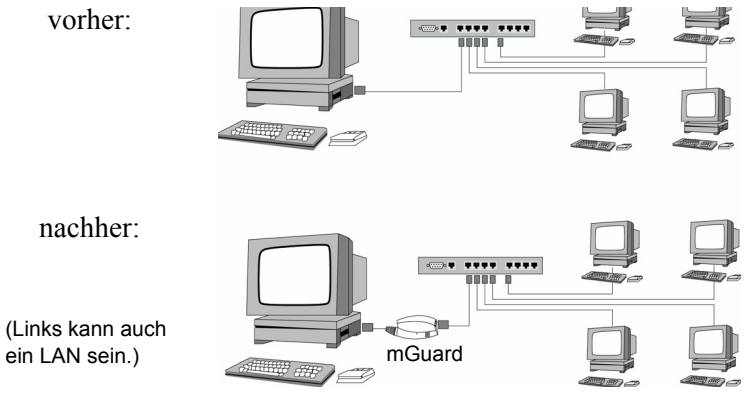
* *Modem / Eingebautes Modem*: Steht nicht bei allen mGuard-Modellen zur Verfügung - siehe „Netzwerk » Interfaces“ auf Seite 109.

Der mGuard muss auf den Netzwerkmodus gestellt werden, der seiner Einbindung in das Netzwerk entspricht. Siehe auch „Typische Anwendungsszenarien“ auf Seite 13.

☞ Je nach dem, auf welchen Netzwerkmodus der mGuard gestellt ist, ändert sich auch die Seite mit den auf ihr angebotenen Konfigurationsparametern.

- **Stealth** *(Werkseinstellung außer mGuard delta und blade Kontroller*)
  Der *Stealth*-Modus wird verwendet, um einen einzelnen Computer oder ein lokales Netzwerk mit dem mGuard zu schützen. Wesentlich ist Folgendes: Ist der mGuard im Netzwerkmodus *Stealth*, wird er in das bestehende Netzwerk

eingefügt (siehe Abbildung), ohne dass die bestehende Netzwerkkonfiguration der angeschlossenen Geräte geändert wird.



Der mGuard analysiert den laufenden Netzwerkverkehr und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent, d. h. ohne dass die Rechner umkonfiguriert werden müssen.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall, Virenschutz und VPN zur Verfügung.

Von extern gelieferte DHCP-Daten werden an den angeschlossenen Rechner durchgelassen.

☞ Eine auf dem Rechner installierte Firewall muss ICMP Echo Requests (Ping) zulassen, wenn der mGuard Dienste wie VPN, DNS, NTP, etc. bereit stellen soll.

☞ Im *Stealth*-Modus hat der mGuard die interne IP Adresse 1.1.1.1, welche vom Rechner erreichbar ist, wenn das auf dem Rechner konfigurierte Standardgateway erreichbar ist.

Im Netzwerkmodus *Stealth* kann zusätzlich ein sekundäres externes Interface konfiguriert werden - siehe „Sekundäres externes Interface (= Extern 2)“ auf Seite 114.

Für die weitere Konfiguration des Netzwerkmodus *Stealth* siehe „» Netzwerk-Modus: Stealth“ auf Seite 120.

- **Router** *(Werkseinstellung mGuard delta und blade Kontroller)*
  Befindet sich der mGuard im *Router*-Modus, arbeitet er als Gateway zwischen verschiedenen Teilnetzen und hat dabei ein externes Interface (= WAN-Port) und ein internes Interface (= LAN-Port) mit jeweils mindestens einer IP-Adresse.

  WAN-Port

  Über seinen WAN-Port ist der mGuard ans Internet oder an Teile des LAN angeschlossen, die als „extern“ gelten.

  - mGuard smart: Der WAN-Port ist die Ethernet-Buchse.

  LAN-Port

  Über seinen LAN-Port ist der mGuard an ein lokales Netzwerk oder an einen Einzelrechner angeschlossen:

  - mGuard smart: Der LAN-Port ist der Ethernet-Stecker.
  - mGuard PCI:
    Im *Treibermodus* wird der LAN-Port durch die Netzwerkschnittstelle des

Betriebssystems gebildet, die das Betriebssystem zur Netzwerkkarte - hier der mGuard PCI - hat.
Im *Power-over-PCI Modus* ist der LAN-Port durch die LAN-Buchse des mGuard PCI gegeben.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall, Virenschutz und VPN zur Verfügung.

☞ Wird der mGuard im *Router*-Modus betrieben, muss er bei lokal angeschlossenen Rechnern als Standardgateway festgelegt sein. D. h. bei diesen Rechnern ist die IP-Adresse des LAN-Ports des mGuard als Adresse des Standardgateway anzugeben.

☞ Wird der mGuard im *Router*-Modus betrieben und stellt die Verbindung zum Internet her, sollte NAT aktiviert werden. Nur dann erhalten die Rechner im angeschlossenen lokalen Netz über den mGuard Zugriff auf das Internet - siehe „Netzwerksicherheit » DoS-Schutz“ auf Seite 188. Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Im Netzwerkmodus *Router* kann zusätzlich ein sekundäres externes Interface konfiguriert werden - siehe „Sekundäres externes Interface (= Extern 2)“ auf Seite 114.

Für die weitere Konfiguration des Netzwerkmodus *Router* siehe „» Netzwerk-Modus: Router“ auf Seite 123.

- **PPPoE**
  Der *PPPoE*-Modus entspricht dem Router-Modus mit DHCP - mit einem Unterschied: Für den Anschluss ans externe Netzwerk (Internet, WAN) wird das PPPoE-Protokoll verwendet, das von vielen DSL-Modems (bei DSL-Internetzugang) verwendet wird. Die externe IP-Adresse, unter der der mGuard von entfernten Gegenstellen aus erreichbar ist, wird vom Provider festgelegt.

  ☞ Wird der mGuard im *PPPoE*-Modus betrieben, muss bei lokal angeschlossenen Rechnern der mGuard als Standardgateway festgelegt sein. D. h. bei diesen Rechnern ist die IP-Adresse des LAN-Ports des mGuard als Adresse des Standardgateway anzugeben.

  ☞ Arbeitet der mGuard im *PPPoE*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten - siehe „Netzwerksicherheit » DoS-Schutz“ auf Seite 188. Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

  Für die weitere Konfiguration des Netzwerkmodus *PPPoE* siehe „» Netzwerk-Modus: PPPoE“ auf Seite 125.

- **PPTP**
  Ähnlich dem *PPPoE*-Modus. In Österreich zum Beispiel wird statt des PPPoE-Protokolls das PPTP-Protokoll zur DSL-Anbindung verwendet.

  (PPTP ist das Protokoll, das ursprünglich von Microsoft für VPN-Verbindungen benutzt worden ist.)

  ☞ Wird der mGuard im *PPTP*-Modus betrieben, muss bei lokal angeschlossenen Rechnern der mGuard als Standardgateway festgelegt sein. D. h. bei diesen Rechnern ist die IP-Adresse des LAN-Ports des mGuard als Standardgateway anzugeben.

☞ Wird der mGuard im *PPTP*-Modus betrieben, sollte NAT aktiviert werden, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten - siehe „Netzwerksicherheit » DoS-Schutz“ auf Seite 188. Ist NAT nicht aktiviert, können eventuell nur VPN-Verbindungen genutzt werden.

Für die weitere Konfiguration des Netzwerkmodus *PPTP* siehe „» Netzwerk-Modus: PPTP“ auf Seite 126.

Nur *mGuard industrial RS*, *mGuard blade, EAGLE mGuard, mGuard delta*

- **Modem**

  Nur bei *mGuard industrial RS* ohne eingebautes Modem, *mGuard blade, EAGLE mGuard, mGuard delta*

  Wird der Netzwerk-Modus *Modem* gewählt, wird die externe Ethernet-Schnittstelle des mGuard deaktiviert, und der Datenverkehr vom und zum WAN läuft über die von außen zugängliche serielle Schnittstelle (Serial Port) des mGuard. An den Serial Port wird ein externes Modem angeschlossen, das die Verbindung ins Telefonnetz herstellt. Die Anbindung ans Internet erfolgt dann (per externem Modem) über das Telefonnetz.

  ⌦ Beim Wechsel des Netzwerk-Modus in oder aus dem *Stealth*-Modus bootet das Gerät automatisch neu.

  ⌦ Wenn Sie die Adresse des mGuard ändern (z. B. durch Wechsel des Netzwerk-Modus von *Stealth* auf *Router*), dann ist das Gerät nur noch unter der neuen Adresse zu erreichen. Erfolgte die Änderung der Konfiguration über den LAN-Port, so erhalten Sie eine Rückmeldung über die neue Adresse, bevor die Änderung aktiv wird. Bei Konfigurationsänderungen über den WAN-Port erhalten Sie keine Rückmeldung.

  ⌦ Wenn Sie den Modus auf *Router* oder *PPPoE* oder *PPTP* stellen und dann die IP-Adresse des LAN-Ports und/oder die lokale Netzmaske ändern, achten Sie unbedingt darauf, dass Sie korrekte Werte angeben. Sonst ist der mGuard unter Umständen nicht mehr erreichbar.

  Für die weitere Konfiguration des Netzwerkmodus *Eingebautes Modem / Modem* siehe „» Netzwerk-Modus: Modem / Eingebautes Modem“ auf Seite 127.

Nur *mGuard industrial RS* mit eingebautem Modem oder eingebautem ISDN-Terminaladapter

- **Eingebautes Modem**

  Nur bei *mGuard industrial RS* mit eingebautem Modem oder ISDN-Terminaladapter

  Wird der Netzwerk-Modus *Eingebautes Modem* gewählt, wird die externe Ethernet-Schnittstelle des mGuard deaktiviert, und der Datenverkehr vom und zum WAN läuft über das im mGuard eingebaute Modem bzw. den eingebauten ISDN-Terminaladapter. Dieses bzw. dieser muss am Telefonnetz angeschlossen sein. Die Anbindung ans Internet erfolgt dann über das Telefonnetz.

  Nach Auswahl von *Eingebautes Modem* werden die Felder zur Festlegung der Parameter für eine Modemverbindung eingeblendet.

  Für die weitere Konfiguration des Netzwerkmodus *Eingebautes Modem / Modem* siehe „» Netzwerk-Modus: Modem / Eingebautes Modem“ auf Seite 127

Sekundäres externes Interface (= Extern 2)

Nur bei *mGuard industrial RS*, *mGuard blade, EAGLE mGuard, mGuard delta*

➔ Nur bei **Netzwerkmodus *Stealth*** oder ***Router.***
Nur bei *mGuard industrial RS*, *mGuard blade, EAGLE mGuard, mGuard delta*:

In diesen Netzwerkmodi kann die serielle Schnittstelle des mGuard als zusätzliches **sekundäres externes Interface** konfiguriert werden.

Über das sekundäre externe Interface kann *permanent* oder *aushilfsweise* Datenverkehr ins externe Netz (WAN) geführt werden.

Bei aktiviertem sekundärem externen Interface gilt Folgendes:

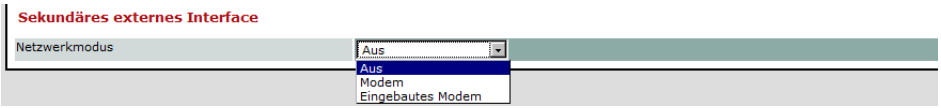
Im Netzwerkmodus *Stealth:*

Nur der vom mGuard erzeugte Datenverkehr wird dem Routing unterzogen, das für das sekundäre externe Interface festgelegt ist, nicht der Datenverkehr, der von einem lokal angeschlossenem Rechner ausgeht. Auch kann auf lokal angeschlossene Rechner nicht von entfernt zugegriffen werden, nur ein Fernzugriff auf den mGuard selber ist - bei entsprechender Konfiguration - möglich.

VPN-Datenverkehr kann - wie im Netzwerkmodus Router - von und zu den lokal angeschlossenen Rechnern fließen. Denn dieser wird vom mGuard verschlüsselt und gilt daher als vom mGuard erzeugt.

Im Netzwerkmodus *Router*:

Alle Datenverkehre, also die von und zu lokal angeschlossenen Rechnern und die, welche vom mGuard erzeugt werden, können über das sekundäre externe Interface ins externe Netz (WAN) geführt werden..



Netzwerkmodus: Aus / Modem / Eingebautes Modem

Aus
(Standard). Wählen Sie diese Einstellung, wenn die Betriebsumgebung des mGuard kein sekundäres externes Interface braucht. Dann können Sie die serielle Schnittstelle (oder das eingebaute Modem - falls vorhanden) für andere Zwecke nutzen - siehe „Modem / Konsole“ auf Seite 139.

Modem / Eingebautes Modem
Bei Auswahl einer dieser Optionen wird der Datenverkehr ins externe Netz (WAN) über das sekundäre externe Interface geführt, entweder *permanent* oder *aushilfsweise*.

Modem:

Das sekundäre externe Interface wird über die serielle Schnittstelle des mGuard und ein daran angeschlossenes externes Modem gebildet.

Eingebautes Modem (nur bei *mGuard industrial RS* mit eingebautem Modem / ISDN-Terminaladapter):

Das sekundäre externe Interface wird über das eingebaute Modem / das eingebaute ISDN-Modem (ISDN-Terminaladapter) gebildet.

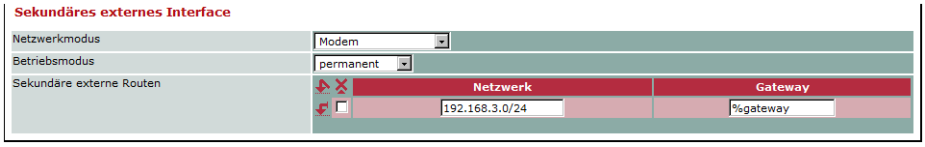
☞ Einstellungen für die Modemverbindung nehmen Sie vor auf der Registerkarte **Ausgehender Ruf** (siehe Seite 131). Unter *Ausgehender Ruf*

legen Sie auch fest, ob die Telefonverbindung bedarfsweise nach Einwahl zur Gegenstelle oder dauerhaft als Standleitung zur Verfügung stehen soll.

☞ Anschlusseinstellungen für ein externes Modem nehmen Sie vor auf der Registerkarte **Modem / Konsole** (siehe Seite 139).

Betriebsmodus: permanent / aushilfsweise

Nach Auswahl des Netzwerkmodus *Modem* oder *Eingebautes Modem* für das sekundäre externe Interface muss der Betriebsmodus des sekundären externen Interface festgelegt werden.



Sowohl in der Betriebsart **permanent** als auch in der Betriebsart **aushilfsweise** muss dem mGuard für das sekundäre externe Interface das Modem zur Verfügung stehen, damit der mGuard über das am Modem angeschlossene Telefonnetz eine Verbindung zum WAN (Internet) herstellen kann.

permanent / aushilfsweise

Welche Datenpakete über das primäre externe Interface (Ethernet-Schnittstelle) und welche Datenpakete über das sekundäre externe Interface gehen, entscheiden die Routing-Einstellungen, die für diese beiden externen Interfaces in Kraft sind. Ein Datenpaket kann also grundsätzlich nur das Interface nehmen, dessen Routing-Einstellung für das vom Datenpaket angesteuerte Ziel passend ist.

- **Für die Anwendung von Routing-Angaben gelten folgende Regeln:**
  - Sind mehrere Routing-Angaben für des Ziel eines Datenpaketes passend, entscheidet das kleinste in den Routing-Angaben definierte Netz, das auf ein Datenpaket-Ziel passt, welche Route dieses Paket nimmt.

    Beispiel:
    Die externe Route des primären externen Interface ist z. B. mit 10.0.0.0/8 angegeben, die externe Route des sekundären externen Interface mit 10.1.7.0/24. Dann werden Datenpakete zum Netz 10.1.7.0/24 über das sekundäre externe Interface geleitet, obwohl für sie die Routing-Angabe für das primäre externe Interface auch passt. Begründung: Die Routing-Angabe für das sekundäre externe Interface bezeichnet ein kleineres Netz (10.1.7.0/24 < 10.0.0.0/8).

    (Diese Regel gilt nicht im Netzwerkmodus *Stealth* in Bezug auf die Stealth Management IP-Adresse - siehe Hinweis unter „Stealth Management IP-Adresse“ auf Seite 120.)
  - Sind die Routing-Angaben für das primäre und das sekundäre externe Interface identisch, dann "gewinnt" das sekundäre externe Interface, d. h. die Datenpakete mit passender Zieladresse werden über das sekundäre externe Interface geleitet.
  - Die Routing-Einstellungen für das sekundäre externe Interface treten nur dann in Kraft, wenn das sekundäre externe Interface aktiviert ist. Das ist insbesondere dann zu berücksichtigen, wenn die Routing-Angaben für des primäre und das sekundäre externe Interface sich

überschneiden oder gleich sind und durch die Priorität des sekundären externen Interface eine Filterwirkung mit folgendem Effekt erzielt wird: Datenpakete, die aufgrund ihres Zieles sowohl für das primäre als auch das sekundäre externe Interface passen, gehen auf jeden Fall über das sekundäre externe Interface, aber nur, wenn dieses aktiviert ist.
"Aktiviert" bedeutet im Betriebsmodus **aushilfsweise** Folgendes: Nur wenn bestimmte Bedingungen erfüllt werden, wird das sekundäre externe Interface aktiviert, und erst dann wirken sich die Routing-Einstellungen des sekundären externen Interface aus.

- Die Netzwerkadresse 0.0.0.0/0 bezeichnet generell das größte definierbare Netz, also das Internet.

☞ Im Netzwerkmodus Router kann das lokale Netz, das am mGuard angeschlossen ist, über das sekundäre externe Interface erreicht werden, sofern die Firewall-Einstellungen so festgelegt sind, dass sie das zulassen.

permanent
Datenpakete, deren Ziel den Routing-Einstellungen entspricht, die für das sekundäre externe Interface festgelegt sind, werden immer über dieses externe Interface geleitet. Das sekundäre externe Interface ist immer aktiviert.

aushilfsweise
Datenpakete, deren Ziel den Routing-Einstellungen entspricht, die für das sekundäre externe Interface festgelegt sind, werden nur dann über dieses externe Interface geleitet, wenn zusätzlich weitere zu definierende Bedingungen erfüllt werden. Nur dann wird das sekundäre externe Interface aktiviert, und die Routing-Einstellungen für das sekundäre externe Interface treten in Kraft - siehe unten unter *Tests zur Aktivierung*.

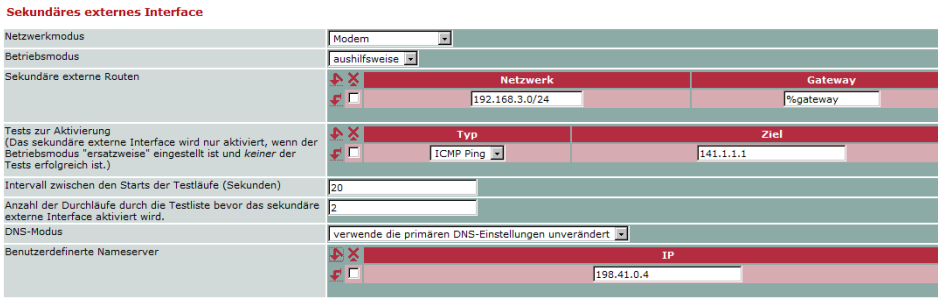
Sekundäre externe Routen

Netzwerk
Machen Sie hier die Angabe für das Routing zum externen Netzwerk. Sie können mehre Routing-Angaben machen. Datenpakete, die für diese Netze bestimmt sind, werden dann über das sekundäre externe Interface zum entsprechenden Netz - *permanent* oder *aushilfsweise* - geleitet.

Gateway
Geben Sie hier die IP-Adresse des Gateways an, über das die Vermittlung in das vorgenannte externe Netzwerk erfolgt - sofern diese IP-Adresse bekannt ist.

Bei Einwahl ins Internet über die Telefonnummer des Internet Service Providers wird die Adresse des Gateways normalerweise erst nach Einwahl bekannt. In diesem Fall ist **%gateway** als Platzhalter in das Feld einzutragen.

Tests zur Aktivierung ...



Ist der Betriebsmodus des sekundären externen Interface auf **aushilfsweise** gestellt, dann wird durch periodisch durchgeführte Ping-Tests Folgendes überprüft: Ist ein bestimmtes Ziel oder sind bestimmte Ziele erreichbar, wenn Datenpakete dorthin ihren Weg aufgrund aller für den mGuard festgelegten Routing-Einstellungen - außer der für das sekundäre externe Interface - nehmen? Nur wenn keiner der Ping-Tests erfolgreich ist, geht der mGuard davon aus, dass es zurzeit nicht möglich ist, das/die Ziel(e) über das primäre externe Interface (= Ethernet-Schnittstelle oder WAN-Port des mGuard) zu erreichen. In diesem Fall wird das sekundäre externe Interface aktiviert, so dass - bei entsprechender Routing-Einstellung für das sekundäre externe Interface - die Datenpakete über dieses Interface geleitet werden.

Das sekundäre externe Interface bleibt so lange aktiviert, bis bei nachfolgenden Ping-Tests der mGuard ermittelt, dass das bzw. die Ziel(e) wieder erreichbar sind. Wird diese Bedingung erfüllt, werden die Datenpakete wieder über das primäre externe Interface geleitet und das sekundäre externe Interface wird deaktiviert.

Die fortlaufend durchgeführten Ping-Tests dienen also dazu zu überprüfen, ob bestimmte Ziele über das primäre externe Interface erreichbar sind. Bei Nichterreichbarkeit wird das sekundäre externe Interface für die Dauer der Nichterreichbarkeit aktiviert.

Typ / Ziel

Legen Sie den Ping-**Typ** des Ping-Request-Pakets fest, das der mGuard zum Gerät mit der IP-Adresse aussenden soll, die Sie unter **Ziel** angeben.

Sie können mehrere solcher Ping-Tests auch zu unterschiedlichen Zielen konfigurieren.

Erfolg / Misserfolg:

Ein Ping-Test gilt dann als erfolgreich absolviert, wenn der mGuard innerhalb von 4 Sekunden eine positive Reaktion auf das ausgesandte Ping-Request Paket erhält. Bei einer positiven Reaktion gilt die Gegenstelle als erreichbar.

Ping-Typen:

IKE Ping:

Ermittelt, ob unter der angegebenen IP-Adresse ein VPN-Gateway erreichbar ist.

ICMP Ping:

Ermittelt, ob unter der angegebenen IP-Adresse ein Gerät erreichbar ist.

Der gebräuchlichste Ping-Test. Die Reaktion auf solche Ping-Tests ist bei manchen Geräten aber ausgeschaltet, so dass sie nicht reagieren, obwohl sie erreichbar sind.

DNS Ping:

Ermittelt, ob unter der angegebenen IP-Adresse ein funktionierender DNS-Server erreichbar ist.

An den DNS-Server mit der angegebenen IP-Adresse wird eine generische Anfrage gerichtet, auf die jeder DNS-Server - sofern erreichbar - eine Antwort gibt.

Bei der Programmierung von Ping-Tests ist Folgendes zu beachten:

Es ist sinnvoll, mehrere Ping-Tests zu programmieren. Denn es könnte sein, dass ein einzelner getesteter Dienst gerade gewartet wird. Solch ein Fall sollte nicht die Auswirkung haben, dass das sekundäre externe Interface aktiviert und eine Kosten verursachende Wählverbindung über das Telefonnetz hergestellt wird.

Da durch die Ping-Tests Netzwerkverkehr erzeugt wird, sollte deren Anzahl und die Häufigkeit ihrer Durchführung angemessen festgelegt werden. Auch sollte vermieden werden, dass das sekundäre externe Interface zu frühzeitig aktiviert wird. Bei den einzelnen Ping-Requests gilt eine Timeout-Zeit von 4 Sekunden. Das bedeutet, dass nach dem Starten eines Ping-Tests der nächste Ping-Test nach 4 Sekunden startet, wenn der vorige negativ war.

Zur Berücksichtigung dieser Aspekte nehmen Sie die nachfolgenden Einstellungen vor.

Intervall zwischen den Starts der Testläufe (Sekunden)

Die oben unter **Tests zur Aktivierung...** definierten Ping-Tests werden nacheinander durchgeführt. Die einmalige sequentielle Durchführung der definierten Ping-Tests wird als *Testlauf* bezeichnet. Testläufe werden in Zeitabständen kontinuierlich wiederholt. Das in diesem Feld angegebene Intervall gibt an, wie lange der mGuard nach dem Start eines Testlaufs abwartet, um den nächsten Testlauf zu starten. Die Testläufe werden nicht unbedingt vollständig abgearbeitet: Sobald ein Ping-Test eines Testlaufs erfolgreich ist, werden die folgenden Ping-Tests desselben Testlaufs ausgelassen. Dauert ein Testlauf länger als das festgelegte Intervall, dann wird der nächste Testlauf direkt im Anschluss gestartet.

Anzahl der Durchläufe durch die Testliste, bevor das sekundäre externe Interface aktiviert wird

Gibt an, wie viele nacheinander durchgeführte Testläufe mit negativem Ausgang es geben muss, damit der mGuard das sekundäre externe Interface aktiviert. Ein Testlauf hat dann einen negativen Ausgang, wenn keiner der darin enthaltenen Ping-Tests erfolgreich war.

Die hier festgelegte Anzahl gibt auch an, wie oft nach Aktivierung des sekundären externen Interface die Testläufe in Folge erfolgreich sein müssen, damit es wieder deaktiviert wird.

DNS-Modus

Nur relevant bei aktiviertem sekundären externem Interface im Betriebsmodus **aushilfsweise**:

Der hier ausgewählte DNS-Modus legt fest, welche DNS-Server der mGuard verwendet für aushilfsweise herzustellende Verbindungen über das sekundäre externe Interface.

Möglichkeiten:

- Verwende die primären DNS-Einstellungen unverändert
- DNS Root Nameserver

- Provider definiert (via PPP-Auswahl)
- Benutzerdefiniert (unten stehende Liste)

Verwende die primären DNS-Einstellungen unverändert

Es werden die DNS-Server benutzt, welche unter Netzwerk --> DNS Server (siehe „Netzwerk » NAT“ auf Seite 145) definiert sind.

DNS Root Nameserver

Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im mGuard gespeichert sind. Diese Adressen ändern sich selten.

Provider definiert (via PPP-Auswahl)

Es werden die Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt.

Benutzerdefiniert (unten stehende Liste)

Ist diese Einstellung gewählt, nimmt der mGuard mit den Domain Name Servern Verbindung auf, die in der nachfolgenden Liste *Benutzerdefinierte Nameserver* aufgeführt sind.

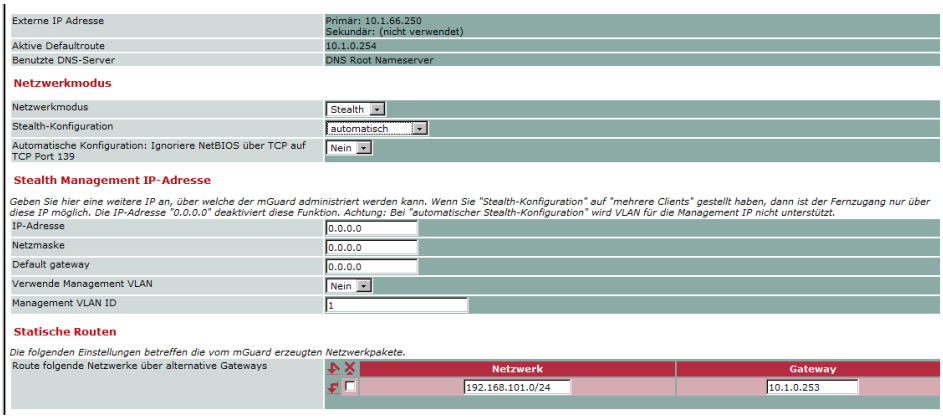
Benutzer definierte Nameserver

In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Diese benutzt der mGuard bei der Kommunikation über das sekundäre externe Interface - sofern dieses aushilfsweise aktiviert ist und der **DNS-Modus** (s. o.) für diesen Fall mit *Benutzerdefiniert* angegeben ist.

» Netzwerk-Modus: Stealth

(Werkseinstellung außer mGuard delta und blade Kontroller)

Wenn als Netzwerk-Modus "Stealth" ausgewählt ist ...



... und für Stealth-Konfiguration "statisch"

Stealth-Konfiguration: automatisch / statisch / mehrere Clients

automatisch

(Standard) Der mGuard analysiert den Netzwerkverkehr, der über ihn läuft, und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig. Er arbeitet transparent.

statisch

Wenn der mGuard keinen über ihn laufenden Netzwerkverkehr analysieren kann, z. B. weil zum lokal angeschlossenen Rechner nur Daten ein-, aber nicht ausgehen, dann muss die *Stealth-Konfiguration* auf **statisch** gesetzt werden. In diesem Fall stellt die Seite unten weitere Eingabefelder zur statischen Stealth-Konfiguration zur Verfügung.

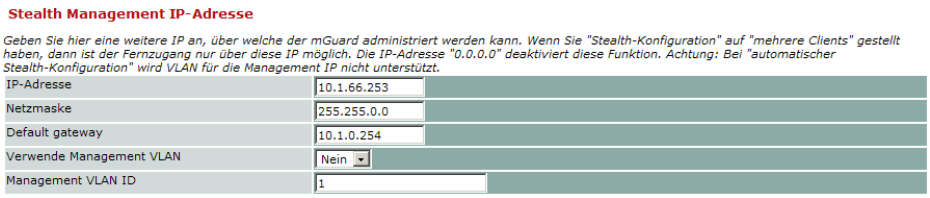
mehrere Clients

Wie bei **automatisch**, es können jedoch mehr als nur ein Rechner am LAN-Port (gesicherter Port) des mGuard angeschlossen sein und somit mehrere IP-Adressen am LAN-Port (gesicherter Port) des mGuard verwendet werden.

Automatische Konfiguration: Ignoriere NetBIOS über TCP auf TCP Port 139: Nein / Ja

Nur bei automatischer Stealth-Konfiguration: Hat ein Windows-Rechner mehr als eine Netzwerkkarte installiert, kann es vorkommen, dass er in den von ihm ausgehenden Datenpaketen abwechselnd unterschiedliche IP-Adressen als Absenderadresse benutzt. Das betrifft Netzwerkpakete, die der Rechner an den TCP Port 139 (NetBIOS) sendet. Da der mGuard aus der Absenderadresse die Adresse des Rechners ermittelt (und damit die Adresse, unter der der mGuard erreichbar ist), müsste der mGuard entsprechend hin- und herschalten, was den Betrieb erheblich stören würde. Um das zu verhindern, setzen Sie diesen Schalter auf **Ja**, sofern Sie den mGuard an einem Rechner angeschlossen haben, der diese Eigenarten aufweist.

Stealth Management IP-Adresse


Stealth Management IP-Adresse
Geben Sie hier eine weitere IP an, über welche der mGuard administriert werden kann. Wenn Sie "Stealth-Konfiguration" auf "mehrere Clients" gestellt haben, dann ist der Fernzugang nur über diese IP möglich. Die IP-Adresse "0.0.0.0" deaktiviert diese Funktion. Achtung: Bei "automatischer Stealth-Konfiguration" wird VLAN für die Management IP nicht unterstützt.
IP-Adresse
10.1.66.253
Netzmaske
255.255.0.0
Default gateway
10.1.0.254
Verwende Management VLAN
Nein
Management VLAN ID
1

Hier können Sie eine weitere IP-Adresse angeben, über welche der mGuard ad-

ministriert werden kann.

Wenn

- unter *Stealth-Konfiguration* die Option **mehrere Clients** gewählt ist oder
- der Client ARP Anfragen nicht beantwortet oder
- kein Client vorhanden ist,

dann ist der Fernzugang über HTTPS, SNMP und SSH nur über diese Adresse möglich.

⌦ Bei *statischer* Stealth-Konfiguration kann die *Stealth Management IP-Adresse* immer erreicht werden, auch wenn der Client-PC seine Netzwerkkarte nicht aktiviert hat.

⌦ Ist das sekundäre externe Interface aktiviert (siehe „Sekundäres externes Interface (= Extern 2)“ auf Seite 114) gilt Folgendes: Sind die Routing-Einstellungen in der Weise in Kraft, dass der Datenverkehr zur **Stealth Management IP-Adresse** über das sekundäre externe Interface geroutet würde, wäre damit eine Ausschlusssituation gegeben, d. h. der mGuard wäre nicht mehr lokal administrierbar. Um das zu verhindern hat der mGuard einen Mechanismus eingebaut, der dafür sorgt, dass in einem solchen Fall die Stealth Management IP-Adresse vom lokal angeschlossenem Rechner (oder Netz) erreichbar bleibt.

IP-Adresse

Die zusätzliche IP-Adresse, unter welcher der mGuard erreichbar und administrierbar sein soll.
Die IP-Adresse „0.0.0.0“ deaktiviert die Management IP-Adresse.

Netzmaske

Die Netzmaske zu obiger IP-Adresse.

Default Gateway

Das Default Gateway (= Standardgateway) des Netzes, in dem sich der mGuard befindet.

Verwende Management VLAN: Ja / Nein

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, so ist diese Option auf **Ja** zu setzen.

Management VLAN ID

Eine VLAN ID zwischen 1 und 4095.

⌦ Bei *automatischer* Stealth-Konfiguration wird VLAN für die Management-IP nicht unterstützt.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich im Glossar auf Seite 279.

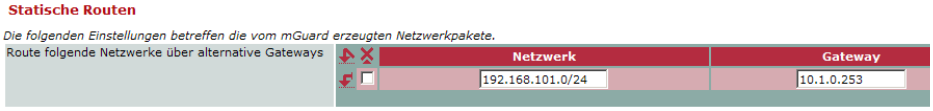
Statische Routen

Im *Stealth*-Modus übernimmt der mGuard das Default Gateway des an seinem LAN-Port angeschlossenen Rechners. Für Datenpakete ins WAN, die der mGuard selber erzeugt, können alternative Routen festgelegt werden. Dazu gehören u. a. die Pakete folgender Datenverkehre:

– das Herunterladen von Zertifikats-Sperrlisten (CRL)
– das Herunterladen einer neuen Konfiguration oder von Virendefinitionsdateien
– die Kommunikation mit einem NTP-Server (zur Zeit-Synchronisation)
– das Versenden und Empfangen verschlüsselter Datenpakete von VPN-Verbindungen

– Anfragen an DNS Server
– Syslog-Meldungen
– das Herunterladen von Firmware-Updates
– das Herunterladen von Konfigurationsprofilen von einem zentralen Server (sofern konfiguriert)
– SNMP-Traps

Soll diese Option genutzt werden, machen Sie nachfolgend die entsprechenden Angaben. Wird sie nicht genutzt, werden die betreffenden Datenpakete über das beim Client festgelegte Default Gateway geleitet.



Netzwerk

Das Netzwerk in CIDR-Schreibweise angeben - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Gateway

Das Gateway, über welches dieses Netzwerk erreicht werden kann.

Die hier festgelegten Routen gelten für Datenpakete, die der mGuard selber erzeugt, als unbedingte Routen. Diese Festlegung hat Vorrang vor sonstigen Einstellungen.

☞ Siehe auch „Netzwerk-Beispielskizze“ auf Seite 264.

Statische Stealth-Konfiguration

IP-Adresse des Clients

Die IP-Adresse des am LAN-Port angeschlossenen Rechner.

MAC-Adresse des Clients

Das ist die physikalische Adresse der Netzwerkkarte des lokalen Rechners, an dem der mGuard angeschlossen ist.

☞ Die MAC-Adresse ermitteln Sie wie folgt:
Auf der DOS-Ebene (Menü Start, Alle Programme, Zubehör, Eingabeaufforderung) folgenden Befehl eingeben:
`ipconfig /all`

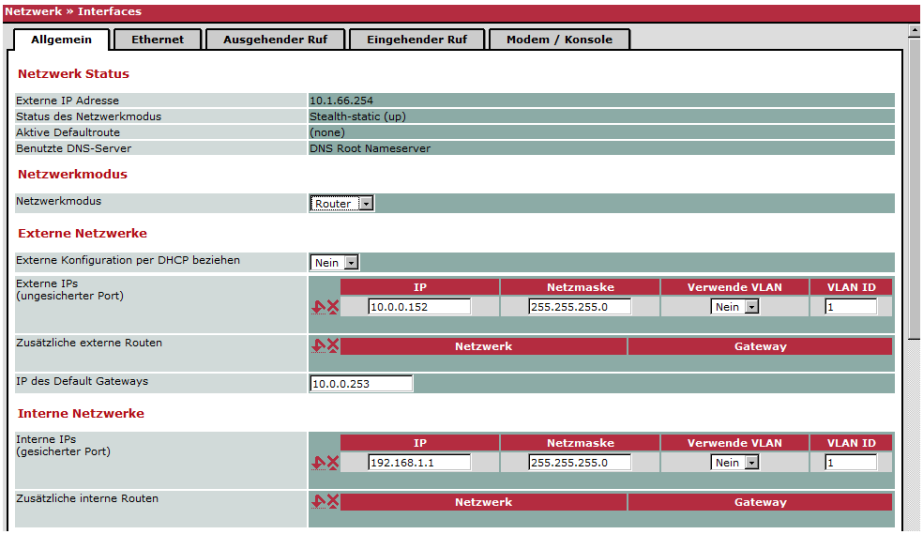
Die Angabe der MAC-Adresse ist nicht unbedingt erforderlich. Denn der mGuard kann die MAC-Adresse automatisch vom Client erfragen. Hierfür muss die MAC-Adresse 0:0:0:0:0:0: eingestellt werden. Zu beachten ist, dass der mGuard aber erst dann Netzwerkpakete zum Client hindurchleiten kann, nachdem er die MAC-Adresse vom Client ermitteln konnte.

Ist im statischen Stealth-Modus weder eine *Stealth Management IP-Adresse* noch die *MAC-Adresse des Clients* konfiguriert, werden DAD ARP Anfragen auf dem internen Interface versendet. (Siehe RFC2131, Abschnitt 4.4.1)

» Netzwerk-Modus: Router

(Werkseinstellung mGuard delta und blade Kontroller)

Wenn als Netzwerk-Modus "Router" ausgewählt ist



Externe Netzwerke (Netzwerkmodus = Router)

Externe Konfiguration per DHCP beziehen: Ja / Nein

☞ Falls der mGuard die Konfigurationsdaten per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Ja** fest. Dann bleiben gegebenfalls weitere bereits bestehende Angaben unter **Externe Netzwerke** wirkungslos, die entsprechenden Felder auf dieser Seite werden ausgeblendet.

☞ Falls der mGuard die Daten nicht per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Nein** fest und machen dann die folgenden Angaben:

Externe IPs (ungesicherter Port)

Die Adressen, unter denen der mGuard von Geräten erreichbar ist, die sich auf Seiten des WAN-Ports befinden. Findet hier der Übergang zum Internet statt, wird die externe IP des mGuard vom Internet Service Provider (ISP) vorgegeben.

⌧ Nur die erste der hier angegebenen externen IP-Adressen wird zur Abwicklung von VPN-Verbindungen verwendet.

IP/Netzmaske

IP-Adresse und Netzmaske des WAN-Ports.

Verwende VLAN: Ja / Nein

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **Ja** zu setzen.

VLAN ID

Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich auf Seite 279.

☞ Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.

Zusätzliche externe Routen

Zusätzlich zur Default Route über das unten angegebene Default Gateway (= Standardgateway) können Sie weitere externe Routen festlegen.

Netzwerk / Gateway

Siehe auch „Netzwerk-Beispielskizze“ auf Seite 264.

IP des Default Gateways

Hier kann die IP-Adresse eines Gerätes im lokalen Netz (angeschlossen am LAN-Port) oder die IP-Adresse eines Gerätes im externen Netz (angeschlossen am WAN-Port) angegeben werden.

Wenn der mGuard den Übergang zum Internet herstellt, wird diese IP-Adresse vom Internet Service Provider (ISP) vorgegeben. Wird der mGuard innerhalb des LANs eingesetzt, wird die IP-Adresse des Default-Gateways vom Netzwerk-Administrator vorgegeben.

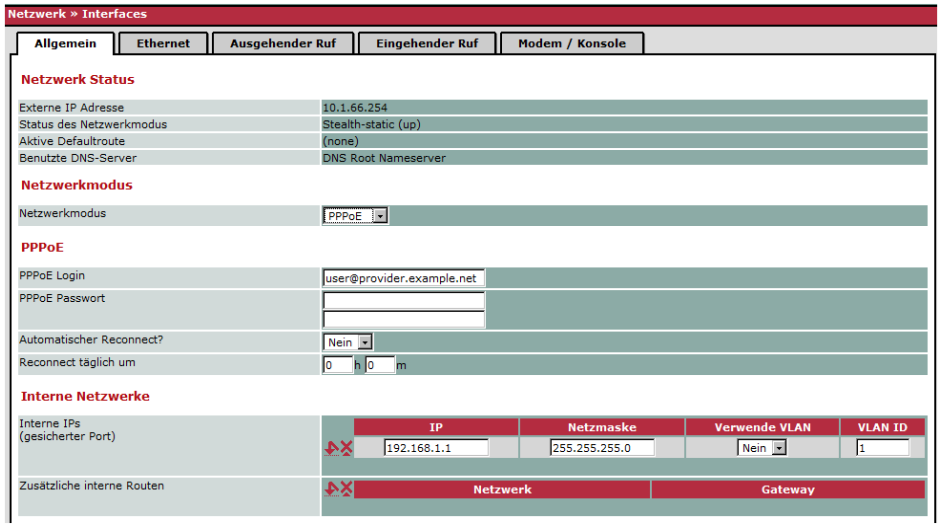
⌦ Wenn das lokale Netz dem externen Router nicht bekannt ist, z. B. im Falle einer Konfiguration per DHCP, dann sollten Sie unter Netzwerksicherheit » NAT Ihr lokales Netz angeben (siehe „Netzwerksicherheit » DoS-Schutz“ auf Seite 188)

Interne Netzwerke

Die Konfiguration der internen Netzwerke ist unter „Netzwerk Modus » Router, PPPoE, PPTP oder Modem / Eingebautes Modem“ auf Seite 128 erklärt.

» Netzwerk-Modus: PPPoE

Wenn als Netzwerk-Modus "PPPoE" ausgewählt ist



PPPoE

Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer einen Benutzernamen (Login) und ein Passwort. Diese werden abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPPoE Login

Benutzername (Login), den der Internet Service Provider (ISP) anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPPoE Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Automatisches Reconnect? Ja / Nein

Bei **Ja** geben Sie im nachfolgenden Feld **Reconnect täglich um** die Uhrzeit an. Dieses Feature dient dazu, das von vielen Internet Providern sowieso erzwungene Trennen und Wiederverbinden mit dem Internet in eine Zeit zu legen, wenn es den Geschäftsbetrieb nicht stört.

Bei Einschalten dieser Funktion greift diese nur dann, wenn die Synchronisation mit einem Zeit-Server erfolgt ist - siehe „Verwaltung » Systemeinstellungen“, „Zeit und Datum“ auf Seite 63.

Reconnect täglich um

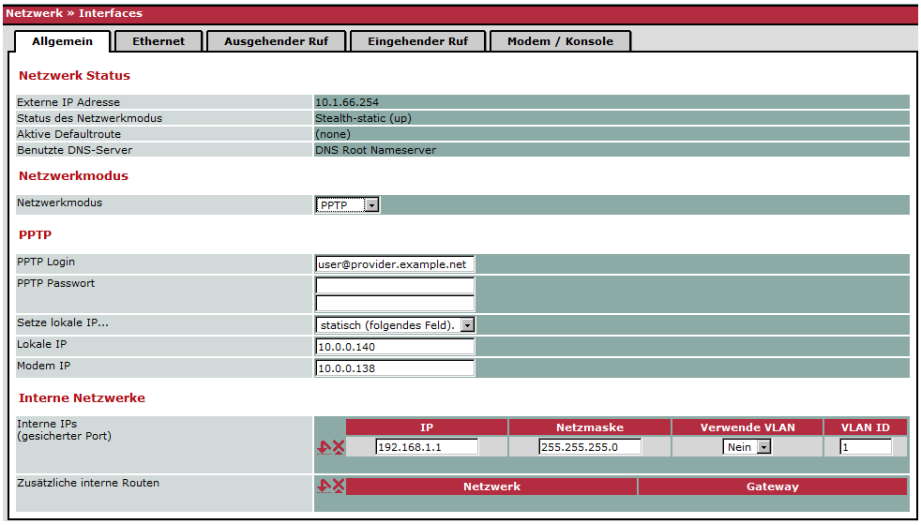
Angabe der Uhrzeit, falls *Automatisches Reconnect* (s. o.) stattfindet.

Interne Netzwerke

Die Konfiguration der internen Netzwerke ist unter „Netzwerk Modus » Router, PPPoE, PPTP oder Modem / Eingebautes Modem“ auf Seite 128 erklärt.

» Netzwerk-Modus: PPTP

Wenn als Netzwerk-Modus "PPTP" ausgewählt ist



PPTP

Für Zugriffe ins Internet gibt der Internet Service Provider (ISP) dem Benutzer einen Benutzernamen (Login) und ein Passwort. Diese werden abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Login

Benutzername (Login), den der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Setze lokale IP...: statisch / über DHCP

Bei über DHCP:

Werden die Adressdaten für den Zugang zum PPTP-Server vom Internet Service Provider per DHCP geliefert, wählen Sie **über DHCP**.

Dann ist kein Eintrag unter **Lokale IP** zu machen.

Bei Statisch (folgendes Feld):

Werden die Adressdaten für den Zugang zum PPTP-Server nicht per DHCP vom Internet Service Provider geliefert, dann muss die lokale IP-Adresse angegeben werden.

Lokale IP

IP-Adresse, unter der der mGuard vom PPTP-Server aus zu erreichen ist.

Modem IP

Das ist die Adresse des PPTP-Servers des Internet Service Providers.

Interne Netzwerke

Die Konfiguration der internen Netzwerke ist unter „Netzwerk Modus » Router, PPPoE, PPTP oder Modem / Eingebautes Modem“ auf Seite 128 erklärt.

» Netzwerk-Modus: Modem / Eingebautes Modem

Nur *mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta*

➔ Der Netzwerk-Modus **Modem** ist verfügbar bei:

mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta.

➔ Der Netzwerk-Modus **Eingebautes Modem** ist zusätzlich verfügbar bei:

mGuard industrial RS, wenn dieser über ein eingebautes Modem oder einen eingebauten ISDN-Terminaladapter verfügt (optional).

Bei allen oben aufgeführten Geräten wird im Netzwerk-Modus *Modem* bzw. *Eingebautes Modem* der Datenverkehr statt über den WAN-Port des mGuard über die serielle Schnittstelle geleitet, und von dort

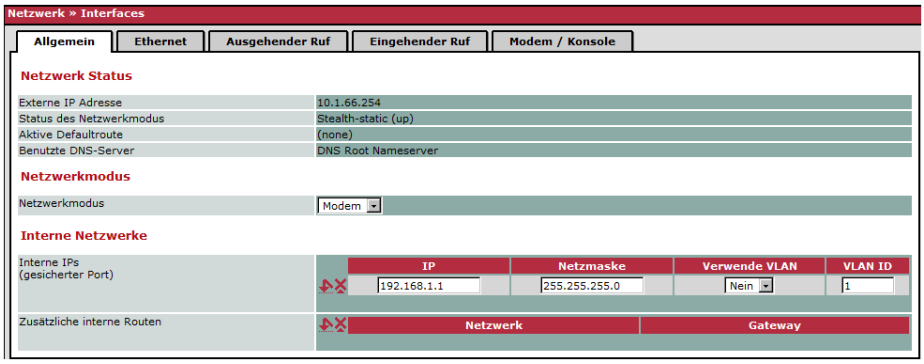
A - entweder über die von außen zugängliche serielle Schnittstelle (Serial Port), an die ein externes Modem angeschlossen werden muss

ODER

B - über das eingebaute Modem / den eingebauten ISDN-Terminaladapter (beim mGuard industrial RS, wenn dieser entsprechend ausgestattet ist).

Sowohl bei Möglichkeit A als auch bei B wird per Modem bzw. ISDN-Terminaladapter über das Telefonnetz die Verbindung zum Internet Service Provider und damit ins Internet hergestellt.

☞ Im Netzwerkmodus *Modem* steht die serielle Schnittstelle des mGuard nicht für für die ppp-Einwahloption und nicht für Konfigurationszwecke zur Verfügung - siehe „Modem / Konsole“ auf Seite 139



Nach Auswahl des Netzwerkmodus **Modem*** geben Sie auf der Registerkarte **Ausgehender Ruf** und/oder **Eingehender Ruf** die für die Modemverbindung erforderlichen Parameter an. Siehe „Ausgehender Ruf“ auf Seite 131 und „Eingehender Ruf“ auf Seite 136.

Auf der Registerkarte ***Modem / Konsole*** nehmen Sie Anschlusseinstellungen für ein externes Modem vor. Siehe „Modem / Konsole“ auf Seite 139.

* Beim mGuard industrial RS auch **Eingebautes Modem** (nur beim mGuard industrial RS mit eingebautem Modem oder ISDN-Terminaladapter - als Option verfügbar).

Die Konfiguration der internen Netzwerke ist im nächsten Abschnitt erklärt.

Netzwerk Modus »
Router, PPPoE, PPTP oder Modem / Eingebautes Modem

Interne Netzwerke

Interne IPs (gesicherter Port)

Interne IP ist die IP-Adresse, unter der der mGuard von Geräten des lokal angeschlossenen Netzes erreichbar ist.

Im **Router**-/**PPPoE**-/**PPTP**-/**Modem**-Modus ist werkseitig voreingestellt:

IP-Adresse:	**192.168.1.1**
Netzmaske:	**255.255.255.0**

Sie können weitere Adressen festlegen, unter der der mGuard von Geräten des lokal angeschlossenen Netzes angesprochen werden kann. Das ist zum Beispiel dann hilfreich, wenn das lokal angeschlossene Netz in Subnetze unterteilt wird. Dann können mehrere Geräte aus verschiedenen Subnetzen den mGuard unter unterschiedlichen Adressen erreichen.

IP
IP-Adresse, unter welcher der mGuard über seinen LAN-Port erreichbar sein soll.

Netzmaske
Die Netzmaske des am LAN-Port angeschlossenen Netzes.

Verwende VLAN
Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **Ja** zu setzen.

VLAN ID
Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ befindet sich im Glossar auf Seite 279.

☞ Falls Sie Einträge aus der Liste löschen wollen: Der erste Eintrag kann nicht gelöscht werden.

Zusätzliche interne Routen

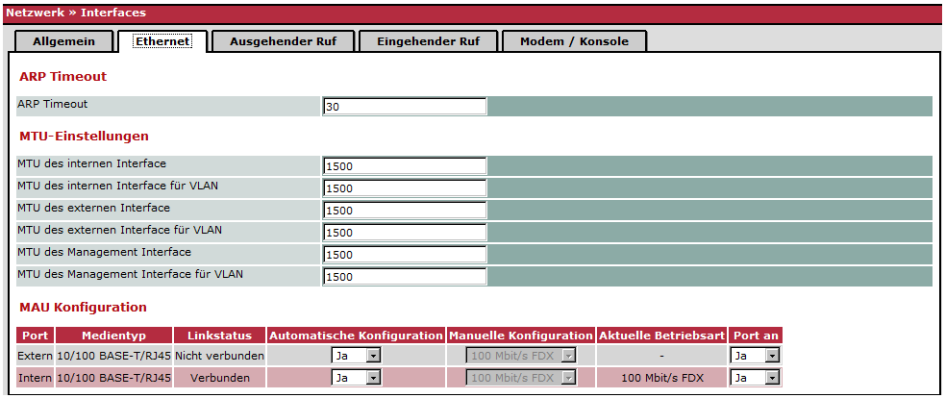
Sind am lokal angeschlossen Netz weitere Subnetze angeschlossen, können Sie zusätzliche Routen definieren.

Netzwerk
Das Netzwerk in CIDR-Schreibweise angeben - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Gateway
Das Gateway, über welches dieses Netzwerk erreicht werden kann.

☞ Siehe auch „Netzwerk-Beispielskizze“ auf Seite 264.

Ethernet



ARP Timeout

ARP Timeout

Lebensdauer der Einträge in der ARP-Tabelle in Sekunden.

MTU Settings

MTU des ... Interface

Die Maximum Transfer Unit (MTU) beschreibt die maximale IP-Paketlänge, die beim betreffenden Interface benutzt werden darf.

⌦ Bei VLAN-Interface:
Da die VLAN Pakete 4 Byte länger als Pakete ohne VLAN sind, haben bestimmte Treiber Probleme mit der Verarbeitung der größeren Pakete. Eine Reduzierung der MTU auf 1496 kann dieses Problem beseitigen.

MAU Konfiguration

Konfiguration und Statusanzeige der Ethernetanschlüsse:

Port

Name des Ethernetanschlusses, auf welchen sich die Zeile bezieht.

Medientyp

Medientyp des Ethernetanschlusses.

Linkstatus

Verbunden: Die Verbindung ist aufgebaut.

Nicht verbunden: Die Verbindung ist nicht aufgebaut.

Automatische Konfiguration: Ja / Nein

Ja: Versuche die benötigte Betriebsart automatisch zu ermitteln.

Nein: Verwende die vorgegebene Betriebsart aus der Spalte „Manuelle Konfiguration“.

⌦ Beim Anschluss des mGuard industrial RS oder des EAGLE mGuard an einen Hub ist Folgendes zu beachten: Bei deaktivierter *Automatischer Konfiguration* wird auch die Auto-MDIX Funktion deaktiviert, d. h. der Port des mGuard industrial RS bzw. EAGLE mGuard muss entweder an den Uplink-Port des Hub oder mittels eines Cross-Link-Kabels mit dem Hub verbunden werden.

Manuelle Konfiguration

Die gewünschte Betriebsart, wenn *Automatische Konfiguration* auf *Nein* gestellt ist.

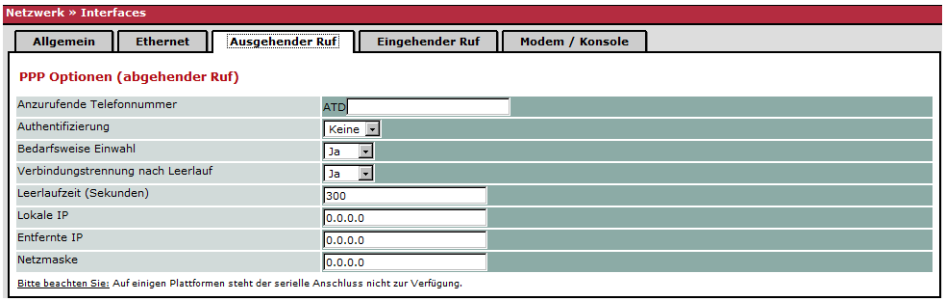
Aktuelle Betriebsart

Die aktuelle Betriebsart des Netzwerkanschlusses.

Port On: Ja / Nein (nur *mGuard industrial RS*, *EAGLE mGuard* **und** *mGuard smart***)**

Schaltet den Ethernetanschluss auf Ein oder Aus.

Ausgehender Ruf



Nur *mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta*

➔ Ist nur dann zu konfigurieren, wenn der mGuard

- über das primäre externe Interface (Netzwerkmodus *Modem* oder *Eingebautes Modem*)

ODER

- über das sekundäre externe Interface (zusätzlich im Netzwerkmodus *Stealth* oder *Router* verfügbar)

eine Datenverbindung ins WAN (Internet) herstellen können soll (Ausgehender Ruf).

PPP Optionen (abgehender Ruf)

Anzurufende Telefonnummer

Telefonnummer des Internet Service Providers. Nach Herstellung der Telefonverbindung wird darüber die Verbindung ins Internet hergestellt.

Befehlssyntax:

Zusammen mit dem bereits vorangestellten Modemkommando ATD zum Wählen ergibt sich für das angeschlossene Modem z. B. folgende Wählsequenz:
`ATD765432`

Standardmäßig wird das kompatiblere Pulswahlverfahren benutzt, das auf jeden Fall funktioniert.

Es können Wählsonderzeichen in die Wählsequenz aufgenommen werden. Siehe dazu die nachfolgende Tabelle:

HAYES-Wählsonderzeichen:

`W` Weist das Modem an, an dieser Stelle eine Wählpause einzulegen, bis das Freizeichen zu hören ist.
Wird verwendet, wenn das Modem an einer Nebenstellenanlage angeschlossen ist, bei der für Anrufe "nach draußen" mit einer bestimmten Nummer (z. B. **`0`**) zunächst das externe Festnetz (das Amt) geholt werden muss und erst dann die Telefonnummer des gewünschten Teilnehmers gewählt werden kann. Beispiel: **`ATD0W765432`**

`T` Wechsel auf Tonwahlverfahren.
Soll bei Anschluss an einen tonwahlfähigen Telefonanschluss das schnellere Tonwahlverfahren verwendet werden, setzen Sie das Wählsonderzeichen **`T`** vor die Rufnummer. Beispiel: **`ATDT765432`**

Authentifizierung: PAP / CHAP / Keine

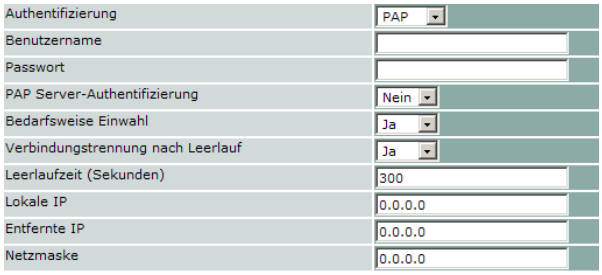
PAP = Password Authentication Protocol, CHAP = Challenge Handshake Authentication Protocol. Das sind Bezeichnungen für Verfahren zur sicheren Übertragung von Authentifizierungsdaten über das Point-to-Point Protocol.

Wenn der Internet Service Provider verlangt, dass sich der Benutzer mit Benutzername und Passwort anmeldet, wird PAP oder CHAP als Authentifizie-

rungsverfahren benutzt. Benutzername und Passwort sowie eventuell weitere Angaben, die der Benutzer für den Aufbau einer Verbindung ins Internet angeben muss, werden dem Benutzer vom Internet Service Provider mitgeteilt.

Je nach dem, ob **PAP** oder **CHAP** oder **Keine** ausgewählt wird, erscheinen unterhalb die entsprechenden Felder. In diese tragen Sie die entsprechenden Daten ein

Wenn die Authentifizierung per PAP erfolgt:



Benutzername

Benutzername, der zur Anmeldung beim Internet Service Provider angegeben werden muss, um Zugang zum Internet zu erhalten.

Passwort

Passwort, das zur Anmeldung beim Internet Service Provider angegeben werden muss, um Zugang zum Internet zu erhalten.

PAP Server-Authentifizierung Ja/Nein

Bei **Ja**:

Die nachfolgen 2 Eingabefelder werden eingeblendet:

Benutzername des Servers

Passwort des Servers

Benutzername und Passwort, die der mGuard beim Server abfragt. Nur wenn der Server die verabredete Benutzernamen/Passwort-Kombination liefert, erlaubt der mGuard die Verbindung.

Nachfolgend aufgeführte Felder

Siehe unter „Wenn als Authentifizierung "Keine" festgelegt wird“ auf Seite 133

Wenn die Authentifizierung per CHAP erfolgt:

Lokaler Name

Ein Name für den mGuard, mit dem er sich beim Internet Service Provider meldet. Eventuell hat der Service Provider mehrere Kunden und muss durch

die Nennung des Namens erkennen können, wer sich bei ihm einwählen will. Nachdem der mGuard sich mit diesem Namen beim Internet Service Provider angemeldet hat, vergleicht der Service Provider dann auch das angegebene *Passwort für die Client-Authentifizierung* (s.u.) Nur wenn der Name dem Service Provider bekannt ist und das Passwort stimmt, kann die Verbindung erfolgreich aufgebaut werden.

Name der Gegenstelle

Ein Name, den der Internet Service Provider dem mGuard nennen wird, um sich zu identifizieren. Der mGuard wird keine Verbindung zum Service Provider aufbauen, wenn dieser nicht den richtigen Namen nennt.

Passwort für die Client-Authentifizierung

Passwort, das zur Anmeldung beim Internet Service Provider angegeben werden muss, um Zugang zum Internet zu erhalten.

CHAP Server-Authentifizierung: Ja/Nein

Bei **Ja**:

Das nachfolge Eingabefeld wird eingeblendet:

Passwort für die Server-Authentifizierung

Passwort, das der mGuard beim Server abfragt. Nur wenn der Server das verabredete Passwort liefert, erlaubt der mGuard die Verbindung.

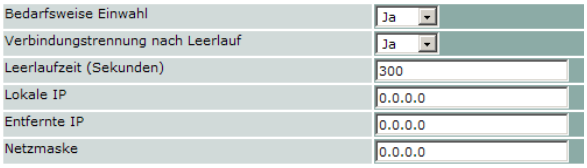
Nachfolgend aufgeführte Felder

Siehe unter „Wenn als Authentifizierung "Keine" festgelegt wird“ auf Seite 133

Wenn als Authentifizierung "Keine" festgelegt wird

In diesem Fall werden die Felder ausgeblendet, die die Authentifizierungsmethoden PAP oder CHAP betreffen.

Es bleiben dann nur die Felder unterhalb sichtbar, die weitere Einstellungen festlegen.



Weitere gemeinsame Einstellungen

Bedarfsweise Einwahl: Ja / Nein

Bei **Ja** (Standard): Diese Einstellung ist sinnvoll bei Telefonverbindungen, deren Kosten nach der Verbindungsdauer berechnet werden.

Der mGuard befiehlt dem Modem erst dann, eine Telefonverbindung aufzubauen, wenn auch wirklich Netzwerkpakete zu übertragen sind. Er weist dann auch das Modem an, die Telefonverbindung wieder abzubauen, sobald für eine bestimmte Zeit keine Netzwerkpakete mehr zu übertragen gewesen sind (siehe Wert in *Verbindungstrennung nach Leerlauf*). Auf diese Weise bleibt

der mGuard allerdings nicht ständig von außerhalb, d. h. für eingehende Datenpakete, erreichbar.

⌧ Der mGuard baut über das Modem auch oft oder sporadisch dann eine Verbindung auf bzw. hält eine Verbindung länger, wenn folgende Bedingungen zutreffen:

- Oft: Der mGuard ist so konfiguriert, dass er seine Systemzeit (Datum und Uhrzeit) regelmäßig mit einem externen NTP-Server synchronisiert.
- Sporadisch: Der mGuard agiert als DNS-Server und muss für einen Client eine DNS-Anfrage durchführen.
- Nach einem Neustart: Eine aktive VPN-Verbindung ist auf **Initiiere** gestellt. Dann wird jedesmal nach einem Neustart des mGuard eine Verbindung aufgebaut.
- Nach einem Neustart: Bei einer aktiven VPN-Verbindung ist das Gateway der Gegenstelle als Hostname angegeben. Dann muss der mGuard nach einem Neustart bei einem DNS-Server die zum Hostnamen gehörige IP-Adresse anfordern.
- Oft: Es sind VPN-Verbindungen eingerichtet und es werden regelmäßig DPD-Nachrichten gesendet (siehe „Dead Peer Detection“ auf Seite 230).
- Oft: Der mGuard ist so konfiguriert ist, dass er seine externe IP-Adresse regelmäßig einem DNS-Service, z. B. DynDNS, mitteilt, damit er unter seinem Hostnamen erreichbar bleibt.
- Oft: Die IP-Adressen von VPN-Gateways von Gegenstellen müssen beim DynDNS-Service angefordert bzw. durch Neuanfragen auf dem aktuellen Stand gehalten werden.
- Sporadisch: Der mGuard ist so konfiguriert, dass SNMP Traps zum entfernten Server gesendet werden.
- Sporadisch: Der mGuard ist so konfiguriert, dass er Fernzugriff per HTTPS, SSH oder SNMP zulässt und annimmt. (Dann sendet der mGuard Antwortpakete an jede IP-Adresse, von der ein Zugriffsversuch erfolgt (sofern die Firewallregeln den Zugriff zulassen würden).
- Oft: Der mGuard ist so konfiguriert, dass er in regelmäßigen Abständen Verbindung zu einem HTTPS Server aufnimmt, um gegebenenfalls ein dort vorliegendes Konfigurationsprofil herunterzuladen. (Siehe „Verwaltung » Zentrale Verwaltung“ auf Seite 102.)

Bei **Nein** baut der mGuard mit Hilfe des angeschlossenen Modems so früh wie möglich nach seinem Neustart oder nach Aktivierung des Netzwerk-Modus *Modem* die Telefonverbindung auf. Diese bleibt dann dauerhaft bestehen, unabhängig davon, ob Daten übertragen werden oder nicht. Wird die Telefonverbindung dennoch unterbrochen, versucht der mGuard, sie sofort wiederherzustellen. So entsteht eine ständige Verbindung, also praktisch eine Standleitung. Auf diese Weise bleibt der mGuard auch ständig von außerhalb, d. h. für eingehende Datenpakete, erreichbar.

⌧ Ob *Ja* oder *Nein*: Es ist immer der mGuard, der die Telefonverbindung aufbaut.

Verbindungstrennung nach Leerlauf: Ja / Nein

Wird nur beachtet, wenn *Bedarfsweise Einwahl* auf **Ja** gestellt ist.

Bei **Ja** (Standard) trennt der mGuard die Telefonverbindung, sobald über die unter *Leerlaufzeit* angegebene Zeitdauer kein Datenverkehr stattfindet. Zur Trennung der Telefonverbindung gibt der mGuard dem angeschlossenen Modem das entsprechende Kommando.

Bei **Nein** gibt der mGuard dem angeschlossenen Modem kein Kommando, die Telefonverbindung zu trennen.

Leerlaufzeit (Sekunden)

Standard: 300. Findet nach Ablauf der hier angegebenen Zeit weiterhin kein Datenverkehr statt, kann der mGuard die Telefonverbindung trennen - siehe oben unter *Verbindungstrennung nach Leerlauf*.

Lokale IP

IP-Adresse der seriellen Schnittstelle des mGuard, die jetzt als WAN-Schnittstelle fungiert. Wird diese IP-Adresse vom Internet Service Provider dynamisch zugewiesen, übernehmen Sie den voreingestellten Wert: 0.0.0.0

Sonst, d. h. bei Zuteilung einer festen IP-Adresse, tragen Sie diese hier ein.

Entfernte IP

IP-Adresse der Gegenstelle. Bei Anbindung ans Internet ist das die IP-Adresse des Internet Service Providers, über die der Zugang ins Internet bereit gestellt wird. Da für die Verbindung das Point-to-Point Protocol (PPP) verwendet wird, muss im Normalfall diese IP-Adresse nicht spezifiziert werden, so dass Sie den voreingestellten Wert übernehmen: 0.0.0.0

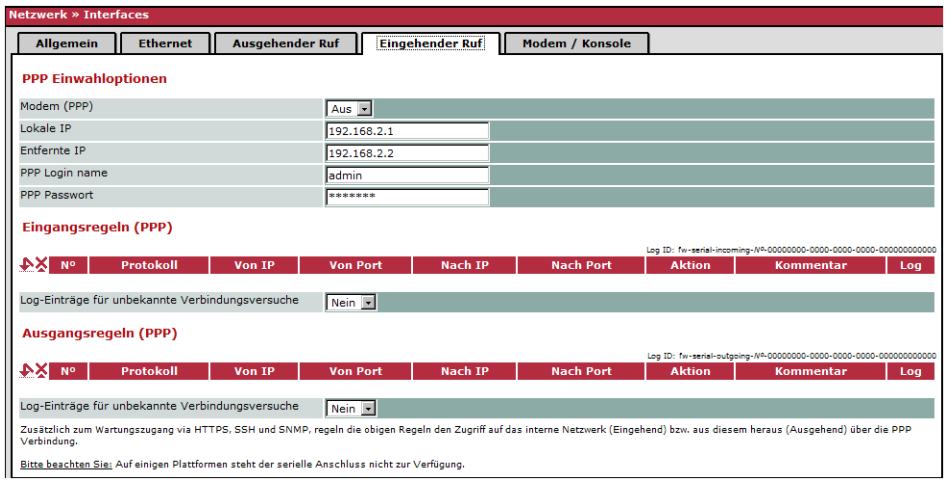
Netzmaske

Die hier anzugegebene Netzmaske gehört zu den beiden IP-Adressen *Lokale IP* und *Entfernte IP*. Üblich ist, dass entweder alle drei Werte (*Lokale IP, Entfernte IP, Netzmaske*) fest eingestellt werden oder auf dem Wert 0.0.0.0 verbleiben.

☞ Auf der Registerkarte ***Modem / Konsole*** nehmen Sie Anschlusseinstellungen für ein externes Modem vor. Siehe „Modem / Konsole“ auf Seite 139.

Eingehender Ruf

Nur *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*



➔ Ist nur dann zu konfigurieren, wenn der mGuard die ppp-Einwahl erlauben soll, entweder über
- ein an der seriellen Schnittstelle angeschlossenes Modem oder
- ein eingebautes Modem (beim mGuard industrial RS als Option verfügbar).

Die ppp-Einwahl kann für Zugriffe ins LAN (oder auf den mGuard für Konfigurationszwecke) genutzt werden - siehe „Modem / Konsole“ auf Seite 139.

☞ Wird das Modem für ausgehende Rufe verwendet, indem es als primäre externe Schnittstelle (Netzwerkmodus *Modem)* des mGuard oder als dessen sekundäre externe Schnittstelle (wenn aktiviert im Netzwerkmodus *Stealth* oder *Router*) fungiert, steht es nicht für die ppp-Einwahloption zur Verfügung.

PPP Einwahloptionen

➔ Bei *mGuard industrial RS* (ohne eingebautes Modem / ISDN-TA), *mGuard blade*, *delta* und *EAGLE mGuard*:

Modem (PPP): Aus / Ein

Der Schalter muss auf **Aus** stehen, wenn keine serielle Schnittstelle für die ppp-Einwahloption genutzt werden soll.

Steht dieser Schalter auf **Ein**, steht die ppp-Einwahloption zur Verfügung. Die Anschlusseinstellungen für das angeschlossene externe Modem sind auf der Registerkarte ***Modem / Konsole*** vorzunehmen.

➔ Bei *mGuard industrial RS* (mit eingebautem Modem oder ISDN-TA):

Modem (PPP): Aus / Eingebautes Modem / Externes Modem

Der Schalter muss auf **Aus** stehen, wenn die serielle Schnittstelle nicht für die ppp-Einwahloption genutzt werden soll.

Steht dieser Schalter auf **Externes Modem**, steht die PPP-Einwahloption zur Verfügung. Dann muss an der seriellen Schnittstelle ein externes Modem angeschlossen sein. Die Anschlusseinstellungen für das angeschlossene externe Modem sind auf der Registerkarte ***Modem / Konsole*** vorzunehmen.

Steht dieser Schalter auf **Eingebautes Modem**, steht die PPP-Einwahloption zur Verfügung. In diesem Fall erfolgt die Modemverbindung nicht über die auf seiner Frontseite befindliche Buchse *Serial* sondern über die Klemmleiste unten, über die das eingebaute Modem bzw. der eingebaute ISDN-Terminaladapter mit dem Telefonnetz verbunden wird. Die Anschlusseinstellungen für

das eingebaute Modem sind auf der Registerkarte ***Modem / Konsole*** vorzunehmen.

Bei Nutzung der Option **Eingebautes Modem** ist es zusätzlich möglich, die serielle Schnittstelle zu benutzen. Zu dessen Nutzungsmöglichkeiten siehe „Modem / Konsole“ auf Seite 139.

Lokale IP

IP-Adresse des mGuard, unter der er bei einer PPP-Verbindung erreichbar ist.

Entfernte IP

IP-Adresse der Gegenstelle von der PPP-Verbindung.

PPP Login name

Anmeldename, welchen die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.

PPP Passwort

Das Passwort, welches die PPP-Gegenstelle angeben muss, um per PPP-Verbindung Zugriff auf den mGuard zu bekommen.

Eingangsregeln (PPP)

Firewallregeln für PPP-Verbindungen zum LAN Interface.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Von / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information über deren Verbleib erhält.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche: Ja / Nein

Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

Ausgangsregeln (Port)

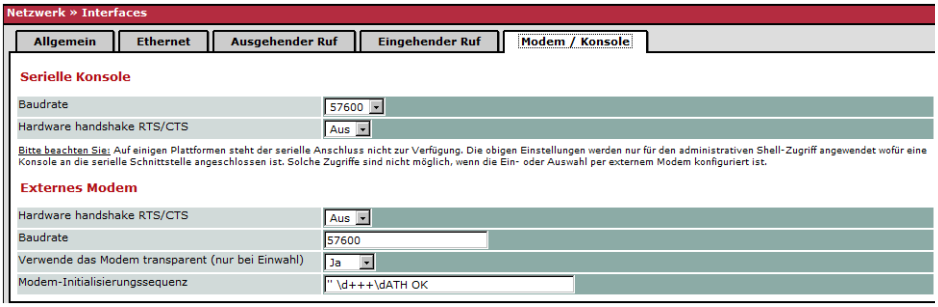
Firewallregeln für ausgehende PPP-Verbindungen vom LAN Interface.

Die Parameter entsprechen denen von *Eingangsregeln (PPP)* - s. o.

Diese Ausgangsregeln gelten für Datenpakete, die bei einer durch PPP-Einwahl initiierten Datenverbindung nach draußen gehen.

Modem / Konsole

Nur *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*


Netzwerk » Interfaces
Allgemein
Ethernet
Ausgehender Ruf
Eingehender Ruf
Modem / Konsole
Serielle Konsole
Baudrate
57600
Hardware handshake RTS/CTS
Aus
Bitte beachten Sie: Auf einigen Plattformen steht der serielle Anschluss nicht zur Verfügung. Die obigen Einstellungen werden nur für den administrativen Shell-Zugriff angewendet wofür eine Konsole an die serielle Schnittstelle angeschlossen ist. Solche Zugriffe sind nicht möglich, wenn die Ein- oder Auswahl per externem Modem konfiguriert ist.
Externes Modem
Hardware handshake RTS/CTS
Aus
Baudrate
57600
Verwende das Modem transparent (nur bei Einwahl)
Ja
Modem-Initialisierungssequenz
" \d+++\dATH OK

Einige mGuard-Modelle verfügen über eine von außen zugängliche serielle Schnittstelle, der mGuard industrial RS optional zusätzlich über ein eingebautes Modem - siehe „Netzwerk » Interfaces“ auf Seite 109.

Nutzungsarten der seriellen Schnittstelle

Die serielle Schnittstelle kann alternativ wie folgt genutzt werden:

- Als primäres externes Interface, wenn unter *Netzwerk* » *Interfaces*, auf der Registerkarte *Allgemein* als Netzwerkmodus ***Modem*** eingestellt ist - siehe „Netzwerk » Interfaces“, „Allgemein“ auf Seite 110. In diesem Fall wird der Datenverkehr nicht über den WAN-Port (= Ethernet-Schnittstelle) abgewickelt, sondern über die serielle Schnittstelle.

ODER

- Als sekundäres externes Interface, wenn unter *Netzwerk* » *Interfaces*, Registerkarte *Allgemein* das ***sekundäre externe Interface*** aktiviert und ***Modem*** ausgewählt ist - siehe „Netzwerk » Interfaces“, „Allgemein“ auf Seite 110. In diesem Fall wird Datenverkehr - permanent oder aushilfsweise - über die serielle Schnittstelle abgewickelt.

ODER

- Für Einwahl ins LAN oder für Konfigurationszwecke. (Siehe auch „Eingehender Ruf“ auf Seite 136.) Es gibt folgende Möglichkeiten:

  A An die serielle Schnittstelle des mGuard ein Modem anschließen, das am Telefonnetz (Festnetz oder GSM-Netz) angeschlossen ist. (Beim mGuard industrial RS mit eingebautem Modem oder ISDN-Terminaladapter erfolgt der Anschluss ans Telefonnetz über die Klemmleiste unten am Gerät.) Dann kann von einem entfernten PC, der ebenfalls mit einem Modem oder ISDN-Adapter am Telefonnetz angeschlossen ist, zum mGuard eine PPP-Wählverbindung (PPP = Point-to-Point Protocol) aufgebaut werden.
  Diese Verwendungsart wird als PPP-Einwahloption bezeichnet. Sie kann für den Zugriff ins LAN benutzt werden, das sich hinter dem mGuard befindet, oder für die Konfiguration des mGuard. In Firewall-Auswahllisten wird für diese Verbindungsart die Interface-Bezeichnung ***Einwahl*** verwendet.
  Damit Sie mit einem Windows-Rechner über die Wählverbindung auf das LAN zugreifen können, muss auf diesem Rechner eine Netzwerkverbindung eingerichtet sein, in der die Wählverbindung zum mGuard definiert ist. Außerdem muss für diese Verbindung die IP-Adresse des mGuard (oder dessen Hostname) als Gateway definiert werden, damit die Verbindungen ins LAN darüber geroutet werden.
  Um auf die Web-Konfigurationsoberfläche des mGuard zuzugreifen, müssen Sie in die Adressenzeile des Web-Browser die IP-Adresse des mGuard (oder dessen Hostname) eingeben.

  B Die serielle Schnittstelle des mGuard mit der seriellen Schnittstelle eines PCs verbinden. Auf dem PC mittels eines Terminalprogramms

die Verbindung zum mGuard herstellen und die Konfiguration über die Kommandozeile des mGuard durchführen.

Sofern an der seriellen Schnittstelle ein externes Modem angeschlossen ist, sind gegebenenfalls weiter unten unter ***Externes Modem*** die passenden Einstellungen zu machen, unabhängig davon, für welche Nutzungsart Sie die serielle Schnittstelle und das an ihr angeschlossene Modem einsetzen.

Serielle Konsole

⌦ Die nachfolgende Einstellungen für *Baudrate* und *Hardware handshake* gelten nur für eine Konfigurationsverbindung, wenn wie oben unter B beschrieben ein Terminal bzw. ein PC mit Terminalprogramm an der seriellen Schnittstelle angeschlossen wird. Nicht gültig, wenn ein externes Modem angeschlossen wird. Die Einstellung dafür erfolgt weiter unten unter ***Externes Modem***.

Baudrate

Über die Auswahlliste können Sie festlegen, mit welcher Übertragungsgeschwindigkeit die serielle Schnittstelle arbeiten soll.

Hardware handshake RTS/CTS: Aus / Ein

Bei **Ein** findet Flusssteuerung durch RTS- und CTS-Signale statt.

Externes Modem

Hardware handshake RTS/CTS: Aus / Ein

Bei **Ein** findet bei der PPP-Verbindungen Flusssteuerung durch RTS- und CTS-Signale statt.

Baudrate

Standard: 57600. Übertragungsgeschwindigkeit für die Kommunikation zwischen mGuard und Modem, die über das serielle Verbindungskabel zwischen den beiden Geräten verläuft.

Der Wert sollte so hoch eingestellt werden, wie es das Modem unterstützt. Ist der Wert niedriger eingestellt als die Geschwindigkeit, welche das Modem auf der Telefonleitung erreichen kann, dann wird die Telefonleitung nicht voll ausgenutzt.

Verwende das Modem transparent (nur bei Einwahl): Ja / Nein

Wird das externe Modem zur Einwahl verwendet (siehe „PPP Einwahloptionen“ auf Seite 136), dann bedeutet die Einstellung **Ja**, dass der mGuard das Modem nicht initialisiert. Die nachfolgend konfigurierte Modem-Initialisierungssequenz wird nicht beachtet. So kann entweder ein Modem angeschlossen werden, das von selbst Anrufe annimmt (Standard-Profil des Modems beinhaltet "Auto-Answer"), oder es kann anstelle des Modems ein Null-Modem-Kabel zu einem Computer und darüber das PPP-Protokoll verwendet werden.

Modem-Initialisierungssequenz

Gibt die Initialisierungssequenz an, die der mGuard zum angeschlossenen Modem sendet.

Standard: `'' \d+++\dATH OK`

Gegebenenfalls im Handbuch zum Modem nachschlagen, wie die Initialisierungssequenz für diese Modem lautet. Die Initialisierungssequenz ist eine Folge von Zeichenketten, die vom Modem erwartet werden, und Befehlen die daraufhin an das Modem gesendet werden, damit das Modem eine Verbindung aufbauen kann.

Die voreingestellte Initialisierungssequenz hat folgende Bedeutung:

`''`	(zwei einfache, direkt hintereinander gesetzte Anführungsstriche) Die leere Zeichenkette inerhalb der Anführungsstriche bedeutet, dass der mGuard am Anfang keine Information vom angeschlossene Modem erwartet, sondern direkt den folgenden Text an das Modem sendet.
`\d+++\dATH`	Diese Zeichenkette sendet der mGuard an das Modem, um dessen Bereitschaft zum Annehmen von Kommandos festzustellen.
`OK`	Gibt an, dass der mGuard vom Modem die Zeichenkette **`OK`** als Antwort auf **`\d+++\dATH`** erwartet.

- Bei vielen Modem-Modellen ist es möglich, Modem-Voreinstellungen im Modem selber abzuspeichern. Doch sollte auf diese Möglichkeit besser verzichtet werden. Notwendige oder gewünschte Initialisierungssequenzen sollten statt dessen lieber extern, d. h. beim mGuard konfiguriert werden. Dann kann bei einem Defekt des Modems dieses schnell und problemlos ausgetauscht werden, ohne auf Modem-Voreinstellungen zu achten.
- Soll das externe Modem für eingehende Rufe verwendet werden, ohne dass die Modem-Voreinstellungen darauf ausgelegt sind, dann müssen Sie dem Modem mitteilen, dass es hereinkommende Rufe nach dem Klingeln annehmen soll. Bei Verwendung des erweiterten HAYES-Befehlssatzes geschieht dies durch das Anhängen der Zeichen „ **`AT&S0=1 OK`**“ (ein Leerzeichen gefolgt von „**`AT&S0=1`**“, gefolgt von einem Leerzeichen, gefolgt von „**`OK`**“) an die Initialisierungssequenz.
- Manches externe Modem benötigt gemäß seiner Werkseinstellungen zur korrekten Funktion die physikalische Verbindung mit der DTR-Leitung der seriellen Schnittstelle. Weil die mGuard-Modelle diese Leitung an der externen seriellen Schnittstelle nicht zur Verfügung stellen, muss dann die obige Initialisierungssequenz um die anzuhängenden Zeichen „ **`AT&D0 OK`**“ (ein Leerzeichen gefolgt von „**`AT&D0`**“, gefolgt von einem Leerzeichen, gefolgt von „**`OK`**“) erweitert werden. Gemäß des erweiterten HAYES-Befehlssatz bedeutet diese Sequenz, dass das Modem die DTR-Leitung nicht verwendet.
- Soll das externe Modem für ausgehende Rufe verwendet werden, ist es an einer Nebenstellenanlage angeschlossen, und erzeugt diese Nebenestellenanlage kein Freizeichen nach dem Abheben, dann muss das Modem angewiesen werden, vor dem Wählen nicht auf ein Freizeichen zu warten. In diesem Fall erweitern sie bitte die Initialisierungssequenz um die anzuhängenden Zeichen „ **`ATX3 OK`**“ (ein Leerzeichen gefolgt von „**`ATX3`**“, gefolgt von einem Leerzeichen, gefolgt von „**`OK`**“). In dem Fall sollten Sie in die „ Anzurufende Telefonnummer“ auf Seite 131 nach der Ziffer zur Amtsholung das Steuerzeichen „**`W`**“ einfügen, damit auf das Freizeichen gewartet wird.

➔ ***mGuard industrial RS* mit eingebautem Modem / eingebautem ISDN-Modem (ISDN-Terminaladapter)**

Der mGuard industrial RS verfügt optional über ein eingebautes Analog-Modem / einen eingebauten ISDN-Terminaladapter. Das eingebaute Modem bzw. der eingebaute ISDN-Terminaladapter kann wie folgt benutzt werden:

- Als primäres externes Interface, wenn unter *Netzwerk* » *Interfaces*, auf der Registerkarte *Allgemein* als Netzwerkmodus ***Eingebautes Modem*** eingestellt ist - siehe „Netzwerk » Interfaces“, „Allgemein“ auf Seite 110. In diesem Fall wird der Datenverkehr nicht über den WAN-Port (= Ethernet-Schnittstelle) abgewickelt, sondern über dieses Modem.

ODER

- Als sekundäres externes Interface, wenn unter *Netzwerk* » *Interfaces*, Registerkarte *Allgemein* das ***sekundäre externe Interface*** aktiviert und ***Eingebautes Modem*** ausgewählt ist - siehe „Netzwerk » Interfaces“, „Allgemein“ auf Seite 110. In diesem Fall wird Datenverkehr auch über die serielle Schnittstelle abgewickelt.

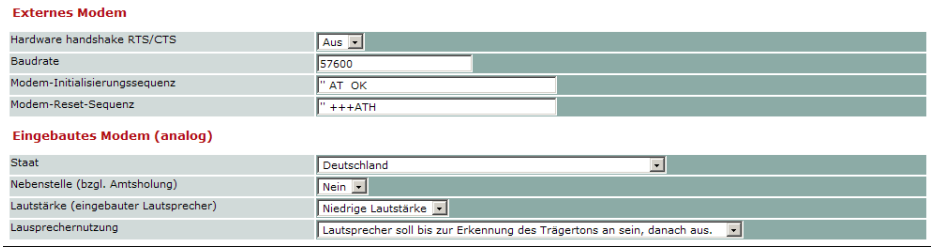
ODER

- für die PPP-Einwahloption (siehe oben unter **Nutzungsarten der seriellen Schnittstelle**)

Beachten Sie, dass die serielle Schnittstelle des Gerätes zusätzlich vergleichbare Nutzungsmöglichkeiten zur Verfügung stellt - siehe oben. So kann beim *mGuard industrial RS* mit eingebautem Modem z. B. der normale Datenverkehr über eine Modemverbindung erfolgen (Netzwerkmodus *Modem*) und gleichzeitig eine zweite Modemverbindung für die PPP-Einwahloption genutzt werden.

Beim *mGuard industrial RS* mit eingebautem Modem

Zusätzlich beim mGuard industrial RS mit eingebautem Modem (analog)



Externes Modem

Wie beim *mGuard industrial RS* (ohne eingebautes Modem), *mGuard blade, EAGLE mGuard* und *mGuard delta:*

Konfiguration wie oben für **Externes Modem** - siehe oben unter „Externes Modem“ auf Seite 140

Eingebautes Modem (analog)

Staat

Hier muss der Staat angegeben werden, in dem der mGuard mit seinem eingebautem Modem betrieben wird. Nur dann ist gewährleistet, dass sich das eingebaute Modem gemäß der in diesem Staat gültigen Fernmeldevorschriften verhält und z. B. Rufton und Wählton richtig erkennt und entsprechend reagiert.

Nebenstelle (bzgl. Amtsholung): Ja / Nein

Bei **Nein** erwartet der mGuard bei Anschaltung ans Telefonnetz den Wählton, wenn der mGuard die Gegenstelle anwählen will.

Bei **Ja** erwartet der mGuard keinen Wählton sondern beginnt gleich mit der Anwahl der Gegenstelle. Dieses Verhalten kann notwendig sein, wenn das eingebaute Modem des mGuard an einer privaten Nebenstellenanlage angeschlossen ist, bei der beim "Abheben" kein Wählton ausgegeben wird. Wenn zur Anwahl nach draußen (Amtsholung) eine bestimmte Nummer, z. B. "0" gewählt werden muss, ist diese der anzuwählenden Telefonnummer der gewünschten Gegenstelle voran zu stellen.

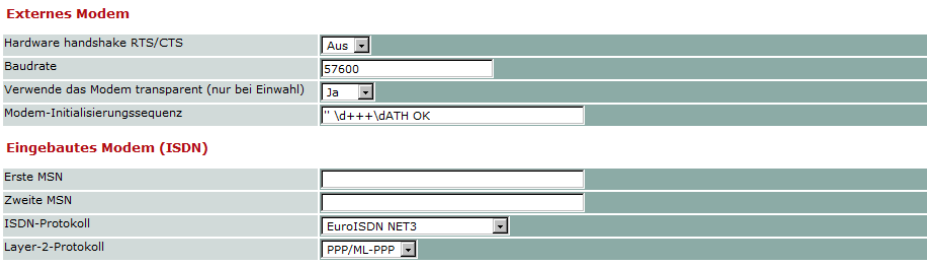
Lautstärke (eingebauter Lautsprecher)

Lautsprechernutzung

Diese beiden Einstellungen legen fest, was der eingebaute Lautsprecher des mGuard wiedergeben soll und in welcher Lautstärke.

Beim *mGuard industrial RS* mit eingebautem ISDN-Terminaladapter

Zusätzlich beim mGuard industrial RS mit eingebautem Modem (ISDN)



Externes Modem

Wie beim *mGuard industrial RS* (ohne eingebautes Modem), *mGuard blade, EAGLE mGuard* und *mGuard delta:*

Konfiguration wie oben für **Externes Modem** - siehe oben unter „Externes Modem“ auf Seite 140

Eingebautes Modem (ISDN)

Erste MSN

Bei ausgehenden Rufen überträgt der mGuard die hier eingetragene MSN (Multiple Subscriber Number) zur angerufenen Gegenstelle. Außerdem ist der mGuard unter dieser MSN für eingehende Anrufe erreichbar (sofern Einwahl ermöglicht ist - siehe Registerkarte ***Allgemein***).

Max. 25 Ziffern/Zeichen; folgende Sonderzeichen können verwendet werden: *****, #, **:** (Doppelpunkt)

Zweite MSN

Soll der mGuard für Einwahl (sofern ermöglicht) zusätzlich unter einer anderen Nummer erreichbar sein, tragen Sie hier eine zweite MSN ein.

ISDN-Protokoll

In Deutschland und vielen anderen europäischen Länder wird das ISDN-Protokoll EuroISDN verwendet, auch NET3 genannt.

Ansonsten ist länderspezifisch festgelegt, welches ISDN-Protokoll benutzt wird. Muss gegebenenfalls bei der zuständigen Telefongesellschaft erfragt werden.

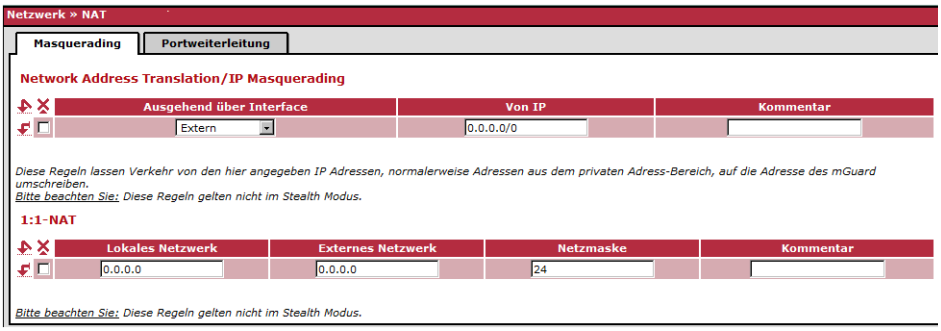
Layer-2-Protokoll

Das Regelwerk, über das sich der ISDN-Terminaladapter des lokalen mGuard mit seiner ISDN-Gegenstelle verständigt. Das ist im Allgemeinen das ISDN-

Modem des Internet Service Providers, über das die Verbindung ins Internet hergestellt wird. Muss beim Internet Service Provider erfragt werden. Sehr häufig wird PPP/ML-PPP verwendet.

6.4.2 Netzwerk » NAT

Masquerading



Network Address Translation / IP Masquerading

Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf.

Das Gerät kann bei ausgehenden Datenpaketen die in ihnen angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird (siehe auch NAT (Network Address Translation) im Glossar).

Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x oder die interne Netzstruktur verborgen werden soll.

Dieses Verfahren wird auch *IP-Masquerading* genannt.

- Arbeitet der mGuard im *PPPoE/PPTP*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.
- Bei der Verwendung von mehreren statischen IP-Adressen für den WAN-Port wird immer die erste IP-Adresse der Liste für IP-Masquerading verwendet.
- im Stealth-Modus werden die Regeln nicht angewendet.

Werkseinstellung: Es findet kein NAT statt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Ausgehend über Interface: Extern / Extern 2 / Alle Externen[1]

Gibt an, über welches Interface die Datenpakete ausgehen, damit sich die Regel auf sie bezieht. Mit **Alle Externen** sind die Interfaces **Extern** und **Extern 2** gemeint.

Von IP

0.0.0.0/0 bedeutet, alle internen IP-Adressen werden dem NAT-Verfahren unterzogen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263

Kommentar

Kann mit kommentierendem Text gefüllt werden.

1. *Extern 2* und *Alle Externen* nur bei Geräten mit serieller Schnittstelle: mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta. Siehe „Sekundäres externes Interface (= Extern 2)“ auf Seite 114.

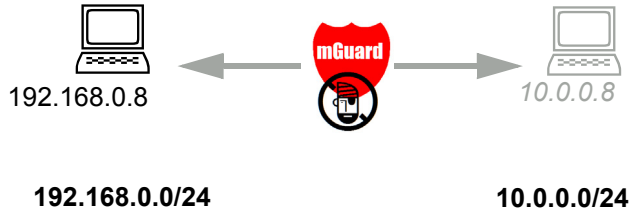
1:1-NAT

Listet die festgelegten Regeln für 1:1-NAT (**N**etwork **A**ddress **T**ranslation) auf.

Bei 1-zu-1 NAT werden die Absender-IP-Adressen so ausgetauscht, dass jede einzelne gegen eine bestimmte andere ausgetauscht wird, und nicht wie beim IP-Masquerading gegen eine für alle Datenpakete identische. So wird ermöglicht, dass der mGuard die Adressen des internen Netzes in das externe Netz spiegeln kann.

Beispiel:

Der mGuard ist über seinen LAN-Port an Netzwerk 192.168.0.0/24 angeschlossen, mit seinem WAN-Port an Netzwerk 10.0.0.0/24. Durch das 1:1 NAT lässt sich der LAN-Rechner 192.168.0.8 im externen Netz unter der IP-Adresse 10.0.0.8 erreichen.



☒ 1:1 NAT kann nicht auf das Interface *Extern 2* angewendet werden.

☒ 1:1 NAT wird nur im Netzwerkmodus *Router* angewendet.

Werkseinstellung: Es findet kein 1:1 NAT statt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Lokales Netzwerk

Die Adresse des Netzwerks am LAN-Port.

Externes Netzwerk

Die Adresse des Netzwerks am WAN-Port.

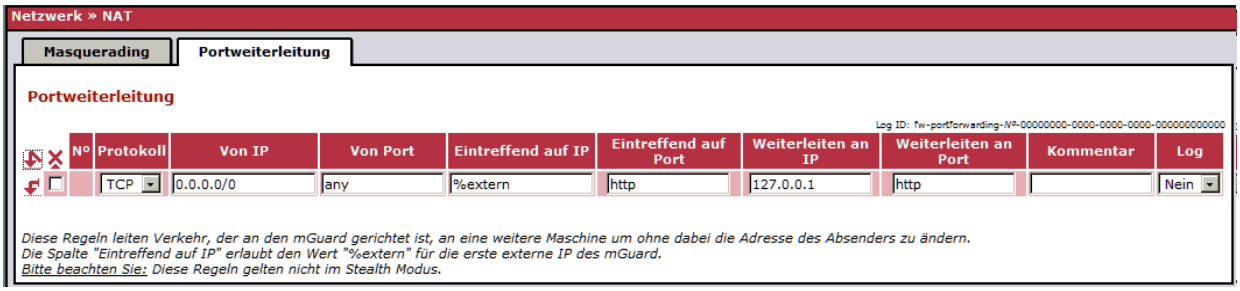
Netzmaske

Die Netzmaske als Wert zwischen 1 und 32 für die lokale und externe Netzwerkadresse (siehe auch „CIDR (Classless Inter-Domain Routing)“ auf Seite 263).

Kommentar

Kann mit kommentierendem Text gefüllt werden.

Portweiterleitung



Listet die festgelegten Regeln zur Port-Weiterleitung (DNAT = Destination-NAT) auf.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuard sowie an einen bestimmten Port des mGuard gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden. D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT genannt.

- Portweiterleitung kann nicht angewendet werden bei Verbindungen, die über das Interface *Extern 2*[1] initiiert werden.
- Die hier eingestellten Regeln haben Vorrang gegenüber den Einstellungen unter **Netzwerk Sicherheit**, **Paketfilter** » **Eingangsregeln**.

Portweiterleitung

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll: TCP / UDP

Geben Sie hier das Protokoll an, auf den sich die Regel beziehen soll.

Von IP

Absenderadresse, für die Weiterleitungen durchgeführt werden sollen.

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Von Port

Absenderport, für den Weiterleitungen durchgeführt werden sollen.

any bezeichnet jeden beliebigen Port.

Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80.

Eintreffend auf IP

Geben Sie hier die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuard an.

ODER

Falls ein dynamischer Wechsel der externen IP-Adresse des mGuard erfolgt, so dass diese nicht angebbar ist, verwenden Sie folgende Variable: **%extern.**

1. *Extern 2* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

⌧ Die Angabe von **%extern** bezieht sich bei der Verwendung von mehreren statischen IP-Adressen für den WAN-Port immer auf die erste IP-Adresse der Liste.

Eintreffend auf Port

Original-Ziel-Port, der in eingehenden Datenpaketen angegeben ist.

Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80.

Weiterleiten an IP

Interne IP-Adresse, an die die Datenpakete weitergeleitet werden sollen und auf die die Original-Zieladressen umgeschrieben werden.

Weiterleiten an Port

Port, an den die Datenpakete weitergeleitet werden sollen und auf den die Original-Port-Angaben umgeschrieben werden.

Er kann entweder über die Port-Nummer oder über den entsprechenden Servicenamen angegeben werden, z. B. *pop3* für Port 110 oder *http* für Port 80.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

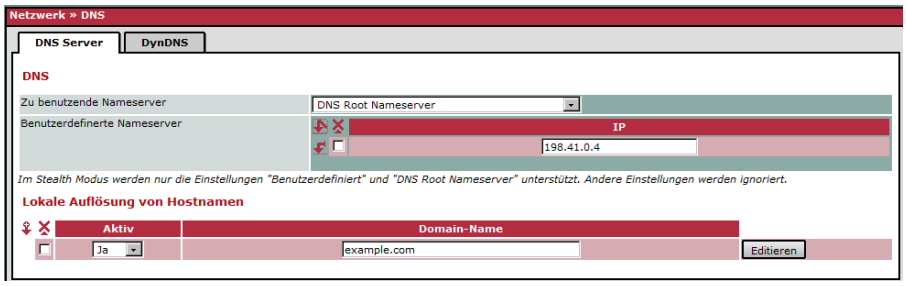
Log

Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

6.4.3 Netzwerk » DNS

DNS Server



Soll der mGuard von sich aus eine Verbindung zu einer Gegenstelle aufbauen (zum Beispiel VPN-Gateway oder NTP-Server) und wird ihm diese in Form eines Hostnamens angegeben (d. h. in der Form www.example.com), dann muss der mGuard ermitteln, welche IP-Adresse sich hinter dem Hostnamen verbirgt. Dazu nimmt er Verbindung zu einem Domain Name Server (DNS) auf, um dort die zugehörige IP-Adresse zu erfragen. Die zum Hostnamen ermittelte IP-Adresse wird im Cache gespeichert, damit sie bei weiteren Hostnamensauflösungen direkt, d. h. schneller gefunden werden kann.

Durch die Funktion *Lokale Auflösung von Hostnamen* kann der mGuard außerdem so konfiguriert werden, dass er selber DNS-Anfragen für lokal verwendete Hostnamen beantwortet, indem er auf ein internes, zuvor konfiguriertes Verzeichnis zugreift.

Die lokal angeschlossenen Clients können (manuell oder per DHCP) so konfiguriert werden, dass als Adresse des zu benutzenden DNS-Servers die lokale Adresse des mGuard verwendet wird. Wird der mGuard im *Stealth*-Modus betrieben, muss bei den Clients die Management-IP-Adresse des mGuard verwendet werden (sofern diese konfiguriert ist), oder es muss die IP-Adresse 1.1.1.1 als lokale Adresse des mGuard angegeben werden.

DNS

Zu benutzende Nameserver

Möglichkeiten:

- DNS Root Nameserver
- Provider-definiert (z. B. via PPPoE oder DHCP)
- Benutzerdefiniert (unten stehende Liste)

DNS Root Nameserver

Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im mGuard gespeichert sind. Diese Adressen ändern sich selten.

Provider-definiert (z. B. via PPPoE oder DHCP)

Es werden die Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. Wählen Sie diese Einstellung nur dann, wenn der mGuard im *PPPoE*-, im *PPTP*-, *Modem*-Modus oder im *Router*-Modus mit DHCP arbeitet.

Benutzerdefiniert (unten stehende Liste)

Ist diese Einstellung gewählt, nimmt der mGuard mit den Domain Name Servern Verbindung auf, die in der Liste *Benutzer definierte Nameserver* aufgeführt sind.

Benutzerdefinierte Nameserver

In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Sollen diesen vom mGuard benutzt werden, muss oben unter **Zu benutzende Nameserver** die Option *Benutzer definiert (unten stehende Liste)* eingestellt sein.

Lokale Auflösung von Hostnamen

Sie können zu verschiedenen Domain-Namen jeweils mehrere Einträge mit Zuordnungspaaren von Hostnamen und IP-Adressen konfigurieren.

Sie haben die Möglichkeit, Zuordnungspaare von Hostnamen und IP-Adressen neu zu definieren, zu ändern (editieren) und zu löschen. Ferner können Sie für eine Domain die Auflösung von Hostnamen aktivieren oder deaktivieren. Und Sie können eine Domain mit all ihren Zuordnungspaaren löschen.

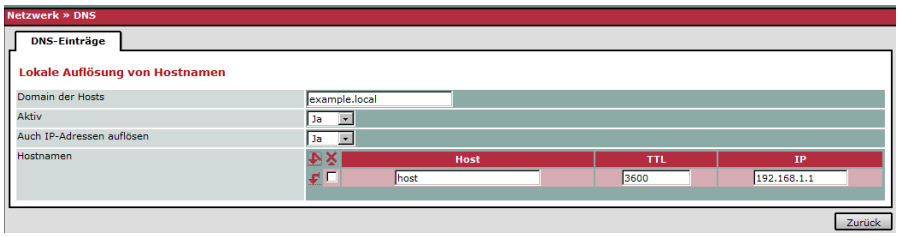
Tabelle mit Zuordnungspaaren für eine Domain anlegen:

Eine neue Zeile öffnen und in dieser auf die Schaltfläche **Editieren** klicken.

Zuordnungspaare, die zu einer Domain gehören, ändern oder löschen:

In der betreffenden Tabellenzeile auf **Editieren** klicken.

Nach Klicken auf die Schaltfläche **Editieren** wird die Registerkarte für *DNS-Einträge* angezeigt:



Domain der Hosts

Der Name kann frei vergeben werden, muss aber den Regeln für die Vergabe von Domain-Namen folgen. Wird jedem Hostnamen zugeordnet.

Aktiv: Ja / Nein

Schaltet die Funktion *Lokale Auflösung von Hostnamen* für die im Feld darüber angegebene Domain auf Ein (**Ja**) oder auf Aus (**Nein**).

Auch IP-Adressen auflösen: Ja / Nein

Nein: Der mGuard löst nur Hostnamen auf, d. h. liefert zu Hostnamen die zugeordnete IP-Adresse.

Ja: Wie bei Nein. Zusätzlich ist es möglich, für eine IP-Adresse die dieser Adresse zugeordneten Hostnamen geliefert zu bekommen.

Hostnamen

Die Tabelle kann beliebig viele Einträge aufnehmen.

☞ Ein Hostname darf mehreren IP-Adressen zugeordnet werden. Einer IP-Adresse dürfen mehrere Hostnamen zugeordnet werden.

TTL

Abkürzung für **T**ime **T**o **L**ive. Angabe in Sekunden. Standard: 3600 (= 1 Stunde)

Gibt an, wie lange abgerufene Zuordnungspaare im Cache des abrufenden Rechners gespeichert bleiben dürfen.

IP

Die IP-Adresse, die dem Hostnamen in dieser Tabellenzeile zugeordnet wird.

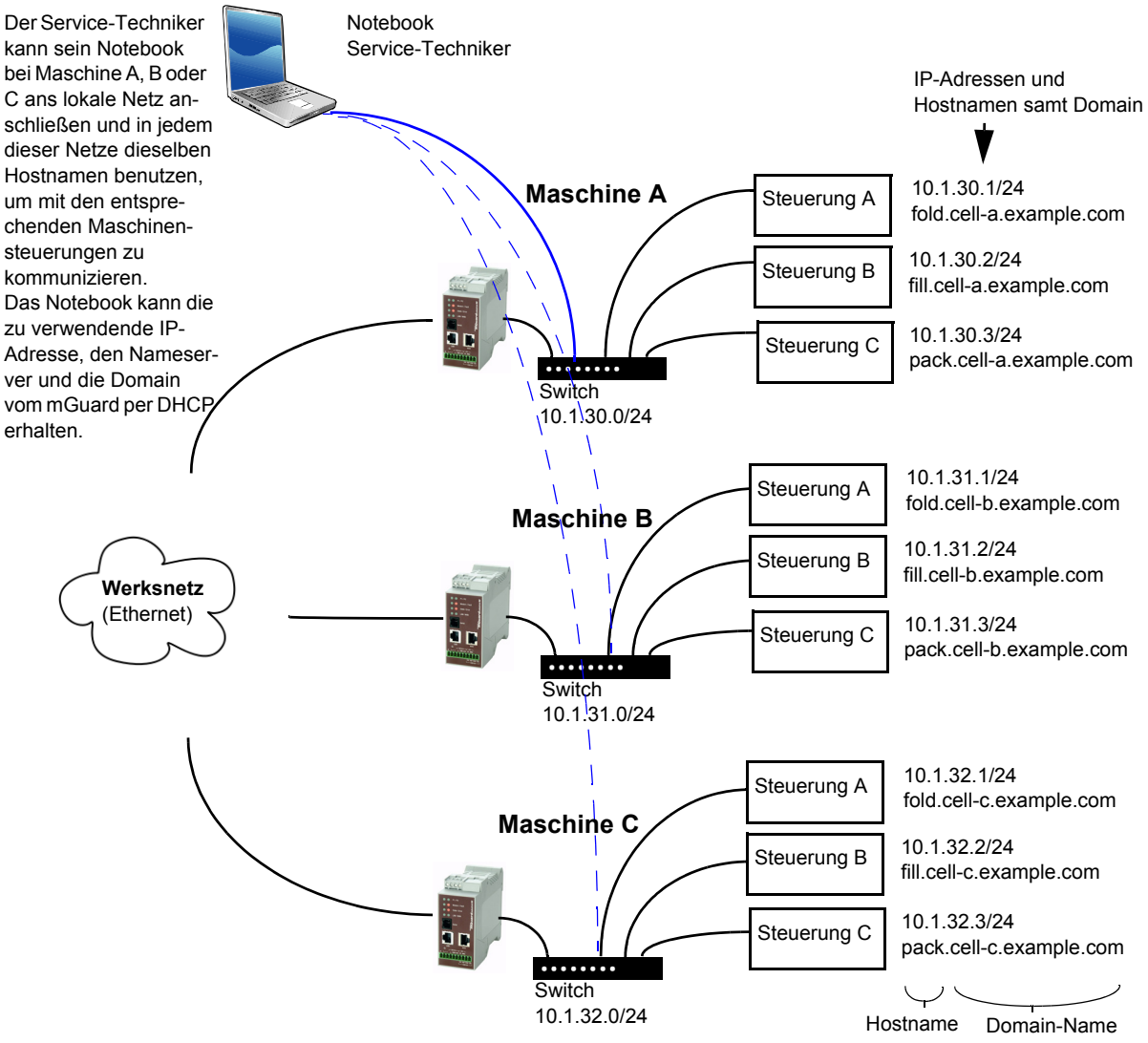
Domäne mit allen Zuordnungspaaren löschen:

Den entsprechenden Tabelleneintrag löschen.

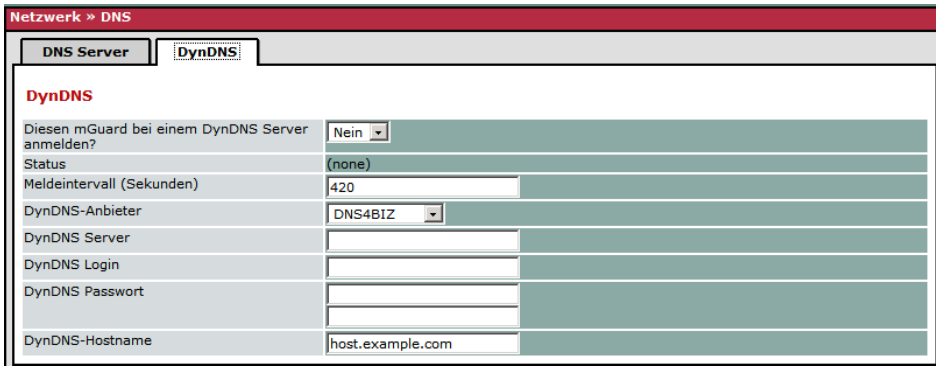
Die Funktion *Lokale Auflösung von Hostnamen* findet z. B. in folgendem Szenario Anwendung:

Ein Werk betreibt mehrere gleich aufgebaute Maschinen, jede als eine sogenannte Zelle. Die lokalen Netze der Zellen A, B und C sind jeweils per mGuard über das Internet mit dem Werksnetz verbunden. In jeder Zelle befinden sich mehrere Steuerungselemente, die über ihre IP-Adressen angesprochen werden können. Dabei werden je Zelle unterschiedliche Adressräume verwendet.

Ein Service-Techniker soll in der Lage sein, sich bei Maschine A, B oder C vor Ort mit seinem Notebook an das dort vorhandene lokale Netz anzuschließen und mit den einzelnen Steuerungen zu kommunizieren. Damit der Techniker nicht für jede einzelne Steuerung in Maschine A, B oder C deren IP-Adresse kennen und eingeben muss, sind den IP-Adressen der Steuerungen jeweils Hostnamen nach einheitlichem Schema zugeordnet, die der Service-Techniker verwendet. Dabei sind die bei den Maschinen A, B und C verwendeten Hostnamen identisch, d. h. zum Beispiel, dass die Steuerung der Verpackungsmaschine in allen drei Maschinen den Hostnamen "pack" hat. Jeder Maschine ist aber ein individueller Domain-Name zugeordnet, z. B. cell-a.example.com.



DynDNS



Zum Aufbau von VPN-Verbindungen muss mindestens die IP-Adresse eines der Partner bekannt sein, damit diese miteinander Kontakt aufnehmen können. Diese Bedingung ist nicht erfüllt, wenn beide Teilnehmer ihre IP-Adressen dynamisch von ihrem Internet Service Provider zugewiesen bekommen. In diesem Fall kann aber ein DynDNS-Service wie z. B. DynDNS.org oder DNS4BIZ.com helfen. Bei einem DynDNS-Service wird die jeweils gültige IP-Adresse unter einem festen Namen registriert.

Sofern Sie für einen vom mGuard unterstützten DynDNS-Service registriert sind, können Sie in diesem Dialogfeld die entsprechenden Angaben machen.

Diesen mGuard bei einem DynDNS Server anmelden? Ja / Nein

Wählen Sie **Ja**, wenn Sie beim DynDNS-Anbieter entsprechend registriert sind, und der mGuard den Service benutzen soll. Dann meldet der mGuard die aktuelle IP-Adresse, die gerade dem eigenen Internet-Anschluss vom Internet Service Provider zugewiesen ist, an den DynDNS Service.

Meldeintervall (Sekunden)

Standard: 420 (Sekunden).

Immer wenn sich die IP-Adresse des eigenen Internet-Anschlusses ändert, informiert der mGuard den DynDNS Service über die neue IP-Adresse. Aus Zuverlässigkeitsgründen erfolgt diese Meldung zusätzlich in dem hier festgelegten Zeitintervall.

Bei einigen DynDNS Anbietern wie z.B. DynDNS.org hat diese Einstellung keine Wirkung, da dort ein zu häufiges Melden zur Löschung des Accounts führen kann.

DynDNS Anbieter

Die zur Auswahl gestellten Anbieter unterstützen das Protokoll, das auch der mGuard unterstützt.

Wählen Sie den Namen des Anbieters aus, bei dem Sie registriert sind, z. B. DynDNS.org, TinyDynDNS, DNS4BIZ

DynDNS Server

Name des Servers des oben ausgewählten DynDNS-Anbieters.

DynDNS Login, DynDNS Passwort

Geben Sie hier den Benutzernamen und das Passwort ein, das Ihnen vom DynDNS-Anbieter zugeteilt worden ist.

DynDNS Hostname

Der für diesen mGuard gewählte Hostname beim DynDNS-Service - sofern Sie einen DynDNS-Dienst benutzen und oben die entsprechenden Angaben

gemacht haben. Unter diesem Hostnamen ist dann Ihr Rechner, der am mGuard angeschlossen ist, erreichbar.

6.4.4 Netzwerk » DHCP

Mit dem Dynamic Host Configuration Protocol (DHCP) kann den direkt am mGuard angeschlossenen Rechner automatisch die hier eingestellte Netzwerkkonfiguration zugeteilt werden. Unter *Internes DHCP* können Sie DHCP Einstellungen für das interne Interface (= LAN-Port) vornehmen und unter *Externes DHCP* die DHCP Einstellungen für das externe Interface (= WAN-Port).

⌧ Der DHCP Server funktioniert auch im *Stealth*-Modus.

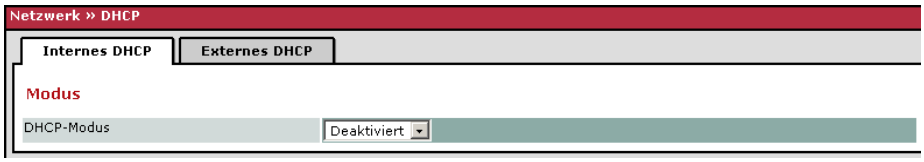
⌧ IP-Konfiguration bei Windows-Rechnern

Wenn Sie den DHCP-Server des mGuard starten, können Sie die lokal angeschlossenen Rechner so konfigurieren, dass sie ihre IP-Adressen automatisch beziehen.

Dazu unter Windows XP **Start, Systemsteuerung, Netzwerkverbindungen**: Das Symbol des LAN-Adapters mit der rechten Maustaste anklicken und im Kontextmenü **Eigenschaften** klicken. Im Dialogfeld *Eigenschaften von LAN-Verbindung* lokales Netz auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren und dann die Schaltfläche **Eigenschaften** klicken.

Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* die gebotenen Angaben bzw. Einstellungen machen.

Internes / Externes DHCP



Modus

DHCP-Modus: Deaktiviert / Server / Relay

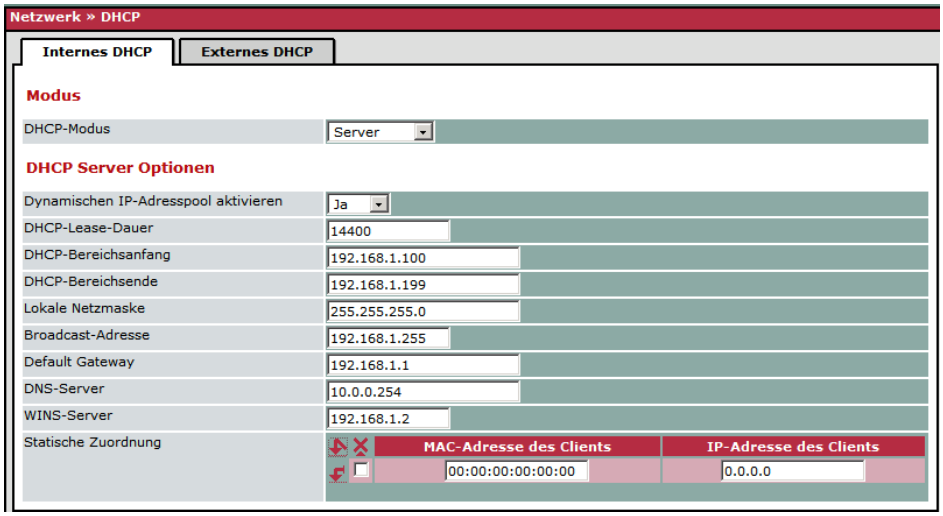
Setzen Sie diesen Schalter auf **Server**, wenn der mGuard als eigenständiger DHCP Server arbeiten soll. Dann werden unten auf der Registerkarte entsprechende Einstellmöglichkeiten eingeblendet - siehe „DHCP-Modus » Server:“ auf Seite 154

Setzen Sie ihn auf **Relay**, wenn der mGuard DHCP Anfragen an einen anderen DHCP Server weiterleiten soll. Dann werden unten auf der Registerkarte entsprechende Einstellmöglichkeiten eingeblendet - siehe „DHCP-Modus » Relay“ auf Seite 155

⌧ Im *Stealth*-Modus des mGuard wird der DHCP-Modus *Relay* nicht unterstützt. Wird der mGuard im *Stealth*-Modus betrieben und ist der DHCP-Modus *Relay* ausgewählt, wird diese Einstellung ignoriert. Aufgrund der Natur des Stealth-Modus werden DHCP-Anfragen des Rechners und die entsprechenden Antworten jedoch durchgeleitet.

Steht der Schalter auf **Deaktiviert**, beantwortet der mGuard keine DHCP Anfragen.

DHCP-Modus » Server:



Ist als DHCP-Modus *Server* ausgewählt, werden unten auf der Seite entsprechende Einstellmöglichkeiten wie folgt eingeblendet.

DHCP Server Optionen

Dynamischen IP-Adresspool aktivieren: Ja / Nein

Setzen Sie diesen Schalter auf **Ja**, wenn sie den weiter unten durch *DHCP-Bereichsanfang* bzw. *DHCP-Bereichsende* angegebenen IP-Adresspool verwenden wollen (siehe unten).

Setzen Sie diesen Schalter auf **Nein**, wenn nur statische Zuweisungen anhand der MAC-Adressen vorgenommen werden sollen (siehe unten).

Bei aktiviertem dynamischen IP-Adresspool:

Bei aktiviertem DHCP-Server und aktiviertem dynamischem IP-Adresspool können Sie die Netzwerkparameter angeben, die vom Rechner benutzt werden sollen:

DHCP-Bereichsanfang: **DHCP-Bereichsende:**	Anfang und Ende des Adressbereichs, aus dem der DHCP-Server des mGuard den lokal angeschlossenen Rechnern IP-Adressen zuweisen soll.

DHCP-Lease-Dauer

Zeit in Sekunden, für die eine dem Rechner zugeteilte Netzwerkkonfiguration gültig ist. Kurz vor Ablauf dieser Zeit sollte ein Client seinen Anspruch auf die ihm zugeteilte Konfiguration erneuern. Ansonsten wird diese u.U. anderen Rechnern zugeteilt.

Lokale Netzmaske

Legt die Netzmaske der Rechner fest. Voreingestellt ist: 255.255.255.0

Broadcast-Adresse

Legt die Broadcast-Adresse der Rechner fest.

Default Gateway

Legt fest, welche IP-Adresse beim Rechner als Default-Gateway benutzt wird. In der Regel ist das die interne IP-Adresse des mGuard.

DNS-Server

Adresse des Servers, bei dem Rechner über den Domain Name Service (DNS) Hostnamen in IP-Adressen auflösen lassen können.

Wenn der DNS-Dienst des mGuard genutzt werden soll, dann die interne IP-Adresse des mGuards angeben.

WINS-Server

Adresse des Servers, bei dem Rechner über den Windows Internet Naming Service (WINS) Hostnamen in Adressen auflösen können.

Statische Zuordnung [anhand der MAC-Adresse]

Die MAC-Adresse Ihres Rechners finden Sie wie folgt heraus:

Windows 95/98/ME: Starten Sie **winipcfg** in einer DOS-Box.
Windows NT/2000/XP: Starten Sie **ipconfig /all** in einer Eingabeaufforderung. Die MAC-Adresse wird als „Physikalische Adresse“ angezeigt.

Linux: Rufen Sie in einer Shell **/sbin/ifconfig** oder **ip link show** auf.

Bei den Angaben haben Sie folgende Möglichkeiten:

MAC-Adresse des Clients

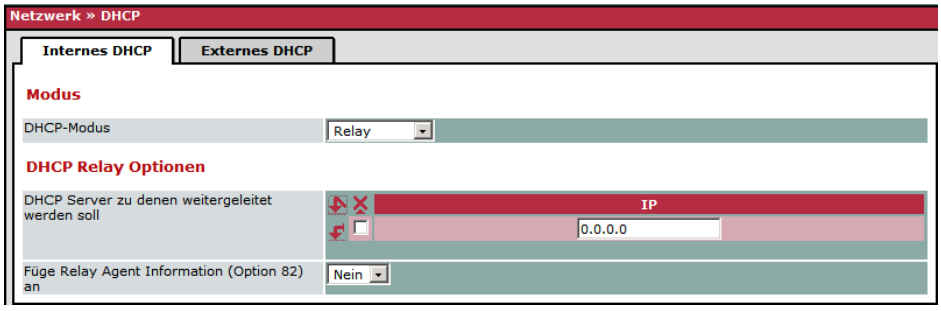
Die MAC-Adresse (ohne Leerzeichen oder Bindestriche) des Rechners.

IP-Adresse des Clients

Die statische IP des Rechners, die der MAC-Adresse zugewiesen werden soll.

- ☞ Die statischen Zuweisungen haben Vorrang vor dem dynamischen IP-Adresspool.
- ☞ Statische Zuweisungen dürfen sich nicht mit dem dynamischen IP-Adresspool überschneiden.
- ☞ Eine IP darf nicht in mehreren statischen Zuweisungen verwendet werden, ansonsten wird diese IP-Adresse mehreren MAC-Adressen zugeordnet.
- ☞ Es sollte nur ein DHCP-Server pro Subnetz verwendet werden.

DHCP-Modus » Relay



Ist als DHCP-Modus *Relay* ausgewählt, werden unten auf der Seite entsprechende Einstellmöglichkeiten wie folgt eingeblendet.

⌦ Im *Stealth*-Modus des mGuard wird der DHCP-Modus *Relay* nicht unterstützt. Wird der mGuard im *Stealth*-Modus betrieben und ist der DHCP-Modus *Relay* ausgewählt, wird diese Einstellung ignoriert. Aufgrund der Natur des Stealth-Modus werden DHCP-Anfragen des Client und die entsprechenden Antworten jedoch durchgeleitet.

DHCP Relay Optionen

DHCP Server, zu denen weitergeleitet werden soll

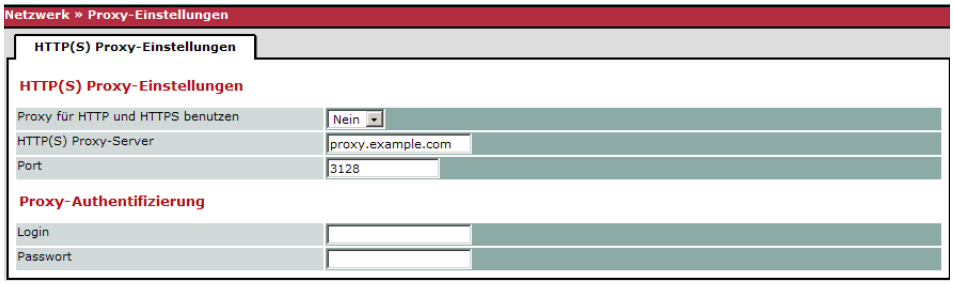
Eine Liste von einem oder mehreren DHCP Servern, an welche DHCP Anfragen weitergeleitet werden sollen.

Füge Relay Agent Information (Option 82) an: Ja / Nein

Beim Weiterleiten können zusätzliche Informationen nach RFC 3046 für die DHCP Server angefügt werden, an welche weitergeleitet wird.

6.4.5 Netzwerk » Proxy-Einstellungen

HTTP(S) Proxy-Einstellungen



Für folgende vom mGuard selbst ausgeführte Aktivitäten kann hier ein Proxy Server angegeben werden:

- CRL-Download
- Firmware-Update
- regelmäßiges Holen des Konfigurationsprofils von zentraler Stelle
- Wiederherstellung von Lizenzen

HTTP(S) Proxy-Einstellungen

Proxy für HTTP und HTTPS benutzen: Ja / Nein

Bei **Ja** gehen Verbindungen, bei denen das Protokoll HTTP oder HTTPS verwendet wird, über einen Proxy Server, dessen Adresse und Port in den nächsten beiden Feldern festzulegen ist.

HTTP(S) Proxy Server

Hostname oder IP-Adresse des Proxy Servers.

Port

Nummer des zu verwendenden Ports, z. B. 3128.

Proxy-Authentifizierung

Login

Benutzername zur Anmeldung beim Proxy Server.

Passwort

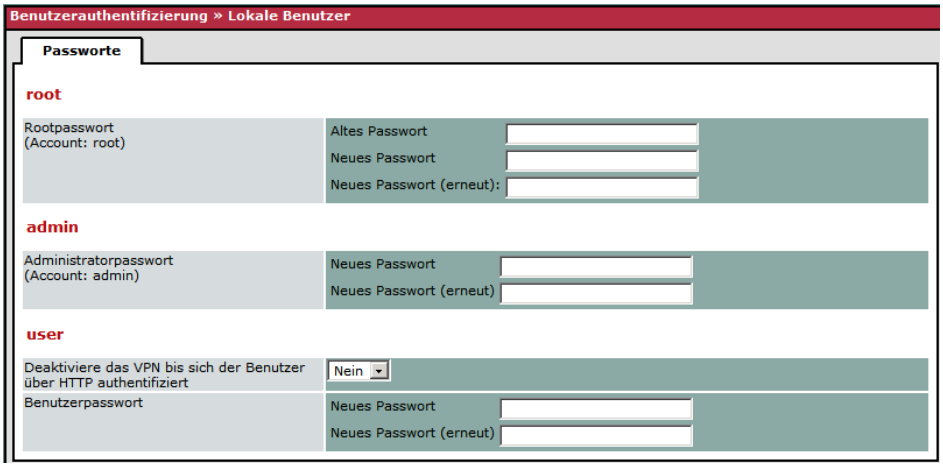
Passwort zur Anmeldung beim Proxy Server.

6.5 Menü Authentifizierung

6.5.1 Authentifizierung » Lokale Benutzer

Unter *lokale Benutzer* sind die Benutzer zu verstehen, die je nach Berechtigungsstufe das Recht haben, den mGuard zu konfigurieren (Berechtigungsstufe *Root* und *Administrator*) oder zu benutzen (Berechtigungsstufe *User*).

Passworte



Um sich auf der entsprechenden Stufe anzumelden, muss der Benutzer das Passwort angeben, das der jeweiligen Berechtigungsstufe zugeordnet ist.

Berechtigungsstufe	
Root	Bietet vollständige Rechte für alle Parameter des mGuard. Hintergrund: Nur diese Berechtigungsstufe erlaubt unbegrenzten Zugriff auf das Dateisystem des mGuards. Benutzername (nicht änderbar):**root** Voreingestelltes Rootpasswort: **root**
Administrator	Bietet die Rechte für die Konfigurationsoptionen, die über die Web-basierte Administratoroberfläche zugänglich sind. Benutzername (nicht änderbar): **admin** Voreingestelltes Passwort: **mGuard**
User	Ist ein Nutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des mGuard bei Zugriff auf eine beliebige HTTP URL dieses Passwort angeben, damit die VPN Verbindungen des mGuard aktiviert werden. Wollen Sie diese Option nutzen, legen Sie im entsprechenden Eingabefeld das Nutzerpasswort fest.

root

Rootpasswort (Account: root)

Werkseitig voreingestellt: **root**

Wollen Sie das Rootpasswort ändern, geben Sie ins Feld *Altes Passwort* das alte Passwort ein, in die beiden Felder darunter das neue gewünschte Passwort.

admin

Administratorpasswort (Account: admin)

Werkseitig voreingestellt: **mGuard**
(unveränderbarer Benutzername: admin)

user

Deaktiviere das VPN bis sich der Benutzer über HTTP authentifiziert: Nein / Ja

Werkseitig ist dieser Schalter auf **Nein** gesetzt.

Bei **Ja** können VPN Verbindungen erst dann genutzt werden, wenn sich ein User mittels HTTP gegenüber dem mGuard ausgewiesen hat.

Alle HTTP Verbindung werden auf den mGuard umgeleitet solange die Authentifizierung erforderlich ist.

Die Änderung dieser Option wird erst mit dem nächsten Neustart aktiv.

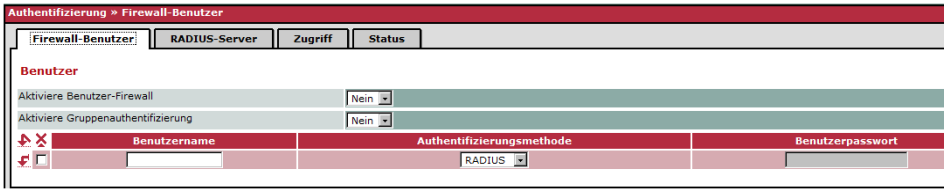
Benutzerpasswort

Werkseitig ist kein Benutzerpasswort voreingestellt. Um eines festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.

6.5.2 Authentifizierung » Firewall-Benutzer

Zum Beispiel um privates Surfen im Internet zu unterbinden, wird unter *Netzwerksicherheit* » *Paketfilter*, *Ausgangsregeln* jede ausgehende Verbindung unterbunden (nicht betroffen: VPN). Unter *Netzwerksicherheit* » *Benutzerfirewall* können für bestimmte Firewall-Benutzer anders lautende Firewall-Regeln definiert werden, z. B. dass für diese jede ausgehende Verbindung erlaubt ist. Diese Benutzerfirewall-Regel greift, sobald sich der oder die betreffende(n) Firewall-Benutzer angemeldet haben, für die diese Benutzerfirewall-Regel gilt, siehe „Netzwerksicherheit » Benutzerfirewall“ auf Seite 190.

Firewall-Benutzer



Benutzer

Listet die Firewall-Benutzer auf durch Angabe der ihnen zugeordneten Benutzernamen. Legt außerdem die Authentifizierungsmethode fest.

Aktiviere Benutzer-Firewall: Ja / Nein

Unter dem Menüpunkt *Netzwerksicherheit* » *Benutzerfirewall* können Firewall-Regeln definiert werden, die dort bestimmten Firewall-Benutzern zugeordnet werden.

Mit **Ja** legen Sie fest, dass die den unten aufgelisteten Benutzern zugeordneten Firewallregeln in Kraft gesetzt werden, sobald sich betreffende Benutzer anmelden.

Aktiviere Gruppenauthentifizierung: Ja / Nein

Wenn aktiviert, leitet der mGuard Logins für ihn unbekannte Benutzer an den RADIUS-Server weiter. Bei Erfolg wird die Antwort des RADIUS-Servers einen Gruppennamen enthalten. Der mGuard wird dann Benutzerfirewall-Templates freischalten, die diesen Gruppennamen als Template Benutzer eingetragen haben.

Der RADIUS-Server muss so konfiguriert werden, dass dieser den Gruppennamen im „Access Accept“ Packet als „Filter-ID=<gruppenname>“ Attribut mitschickt.

Benutzername

Name, den der Benutzer angeben muss, wenn er sich anmeldet.

Authentifizierungsmethode: RADIUS / Local DB

Local DB:

Ist *Local DB* ausgewählt, muss in der Spalte *Benutzerpasswort* das Passwort eingetragen werden, das dem Benutzer zugeordnet ist, und das dieser neben seinem *Benutzernamen* angeben muss, wenn er sich anmeldet.

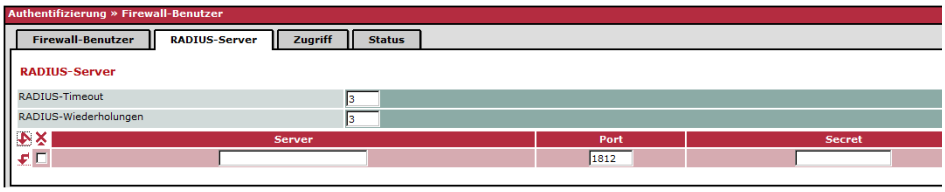
Radius:

Ist RADIUS ausgewählt, kann das Passwort für den Benutzer auf dem RADIUS-Server hinterlegt werden.

Benutzerpasswort

Nur aktiv, wenn als Authentifizierungsmethode Local DB ausgewählt ist.

RADIUS-Server



RADIUS-Server

RADIUS-Timeout

Legt fest (in Sekunden), wie lange der mGuard auf die Antwort des RADIUS-Servers wartet. Standard: 3 Sekunden

RADIUS-Wiederholungen:

Legt fest, wie oft bei Überschreitung des RADIUS-Timeout Anfragen an den Radius-Server wiederholt werden. Standard: 3

Server

Name des RADIUS-Servers oder dessen IP-Adresse

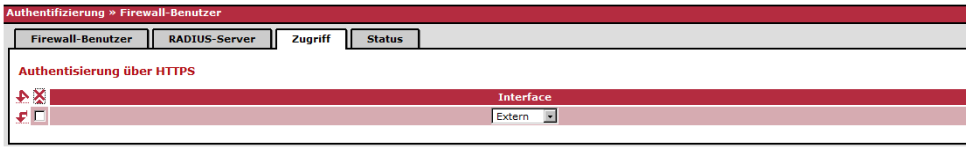
Port

Vom RADIUS-Server benutze Port-Nummer

Secret

RADIUS-Server-Passwort

Zugriff



Authentisierung über HTTPS

Interface: Extern / Intern / Extern 2 / Einwahl[1]

Gibt an, über welche mGuard-Interfaces Firewall-Benutzer sich beim mGuard anmelden können. Für das ausgewählte Interface muss Web-Zugriff über HTTPS freigeschaltet sein: Menü **Verwaltung**, **Web-Einstellungen**, Registerkarte ***Zugriff***. Siehe „Zugriff“ auf Seite 75.

☞ Im Netzwerkmodus *Stealth* müssen sowohl das Interface **Intern** als auch das Interface **Extern** freigeschaltet werden, damit Firewall-Benutzer sich beim mGuard anmelden können. (Dazu müssen also 2 Zeilen in die Tabelle aufgenommen werden.)

⌦VORSICHT:

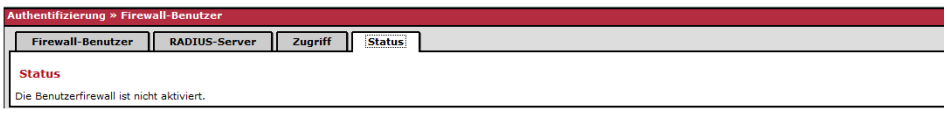
Bei Authentisierung über ein externes Interface ist Folgendes zu bedenken: Kann sich ein Firewall-Benutzer über ein "unsicheres" Interface einloggen,

1. *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

könnte es passieren, dass bei einer Trennung ohne ordnungsgemäßes Ausloggen das Login bestehen bleibt und von einer anderen, nicht berechtigten Person missbraucht wird. "Unsicher" ist das Interface z. B. dann, wenn sich ein Benutzer über das Internet einloggt von einer Stelle oder einem Rechner, der/dem die IP-Adresse vom Internet Service Provider dynamisch zugeordnet wird - wie es bei vielen Internet-Benutzern üblich ist. Kommt es während einer solchen Verbindung z. B. zu einer kurzzeitigen Zwangstrennung, weil dem eingeloggten Benutzer gerade eine andere IP-Adresse zugeordnet wird, dann muss sich dieser Benutzer neu einloggen. Das alte Login, dass er unter seiner alten IP-Adresse vollzogen hat, bleibt aber bestehen, so dass dieses Login von einem Eindringling benutzt werden könnte, der diese "alte" IP-Adresse des rechtmäßigen Benutzers für sich verwendet und unter dieser Absender-Adresse auf den mGuard zugreift. Entsprechendes könnte auch geschehen, wenn ein (befugter) Firewall-Benutzer vergisst, sich nach der Sitzung auszuloggen.

Diese Unsicherheit beim Einloggen über ein "unsicheres Interface" wird zwar nicht grundsätzlich beseitigt, aber zeitlich eingegrenzt, indem für das verwendete Benutzerfirwall-Template das konfigurierte Timeout gesetzt ist.
Siehe „ Timeout Typ: statisch / dynamisch“ auf Seite 191.

Status



Bei aktivierter Benutzerfirewall wird hier deren Status angezeigt.

6.5.3 Authentifizierung » Zertifikate

Begriffsdefinitionen

Der Nachweis und die Prüfung der Authentizität, Authentifizierung genannt, ist grundlegendes Element einer sicheren Kommunikation. Beim X.509 Authentifizierungsverfahren wird anhand von Zertifikaten sichergestellt, dass wirklich die "richtigen" Partner kommunizieren und kein "falscher" dabei ist. Falsch wäre ein Kommunikationspartner dann, wenn er vorgibt, jemand zu sein, der er in Wirklichkeit gar nicht ist, siehe Glossar unter "X.509-Zertifikat".

Zertifikat

Ein Zertifikat dient dem Zertifikatsinhaber als Bescheinigung dafür, dass er der ist, für den er sich ausgibt. Die bescheinigende, beglaubigende Instanz dafür ist die CA (Certificate Authority). Von ihr stammt die Signatur (= elektronische Unterschrift) auf dem Zertifikat, mit der die CA bescheinigt, dass der rechtmäßige Inhaber des Zertifikats einen privaten Schlüssel besitzt, der zum öffentlichen Schlüssel im Zertifikat passt.

Der Name des Ausstellers eines Zertifikats wird im Zertifikat als *Issuer* aufgeführt, der Name des Inhabers eines Zertifikats als *Subject*.

Selbst signierte Zertifikate

Ist ein Zertifikat nicht von einer CA (Certificate Authority) signiert, sondern vom Zertifikatsinhaber selber, spricht man von einem selbst signierten Zertifikat. In selbst signierten Zertifikaten wird der Name des Zertifikatsinhabers sowohl als *Issuer* als auch als *Subject* aufgeführt.

Selbst signierte Zertifikate werden benutzt, wenn die Kommunikationspartner den Vorgang der X.509-Authentifizierung verwenden wollen oder müssen, ohne ein offizielles Zertifikat zu haben oder zu benutzen. Diese Art der Authentifizierung sollte aber nur unter Kommunikationspartnern Verwendung finden, die sich "gut kennen" und deswegen vertrauen. Sonst sind solche Zertifikate unter dem Sicherheitsaspekt genauso wertlos wie z. B. selbst erstellte Ausweispapiere, die keinen Behördenstempel tragen.

Zertifikate werden von kommunizierenden Maschinen / Menschen bei der Verbindungsaufnahme einander "vorgezeigt", sofern zur Verbindungsaufnahme die X.509-Authentifizierung verwendet wird. Beim mGuard können das die folgenden Anwendungen sein:

- Authentifizierung der Kommunikationspartner bei der Herstellung von VPN-Verbindungen - siehe „IPsec VPN » Verbindungen“, „Authentifizierung“ auf Seite 222
- Verwaltung des mGuard per SSH (Shell Zugang) - siehe „Verwaltung » Systemeinstellungen“, „Shell-Zugang“ auf Seite 67
- Verwaltung des mGuard per HTTPS- siehe „Verwaltung » Web Einstellungen“, „Zugriff“ auf Seite 75

Zertifikat, Maschinenzertifikat

Mit Zertifikaten kann man sich gegenüber anderen ausweisen (sich authentisieren). Das Zertifikat, mit dem sich der mGuard gegenüber anderen ausweist, soll hier, der Terminologie von Microsoft Windows folgend, "Maschinenzertifikat" genannt werden.

Wird ein Zertifikat von einem Menschen benutzt, um sich gegenüber Gegenstellen zu authentisieren (z. B. von einem Menschen, der per HTTPS und Web-Browser auf den mGuard zwecks Fernkonfiguration zugreifen will), spricht man einfach von Zertifikat, personenbezogenem Zertifikat oder Benutzerzertifikat, das dieser Mensch "vorzeigt". Ein solches personenbezogenes Zertifikat kann z. B. auch auf einer Chipkarte gespeichert sein und von dessen Inhaber bei Bedarf in den Kartenleser seines Rechners gesteckt werden, wenn der Web-Browser bei der Verbindungsherstellung dazu auffordert.

Gegenstellen-zertifikat

Ein Zertifikat wird also von dessen Inhaber (Mensch oder Maschine) wie ein Ausweis benutzt, nämlich um zu "beweisen", dass er/sie wirklich der/die ist, für den er/sie sich ausgibt. Weil es bei einer Kommunikation mindestens zwei Partner gibt, geschieht das wechselweise: Partner A zeigt sein Zertifikat seiner Gegenstelle, Partner B, vor. Und Partner B zeigt sein Zertifikat seiner Gegenstelle vor, Partner A.

Damit A das ihm von B vorgezeigte Zertifikat, also das Zertifikat seiner Gegenstelle, akzeptieren und die Kommunikation mit B erlauben kann, gibt es folgende Möglichkeit: A hat zuvor von B eine Kopie des Zertifikats erhalten (z. B. per Datenträger oder E-Mail), mit dem sich B bei A ausweisen wird. Anhand eines Vergleiches mit dieser Kopie kann A dann erkennen, dass das von B vorgezeigte Zertifikat zu B gehört. Die Kopie des Zertifikats, das in diesem Beispiel Partner B an A übergeben hatte, nennt man (auf die Oberfläche des mGuard bezogen) *Gegenstellenzertifikat*.

Damit die wechselseitige Authentifizierung gelingen kann, müssen also zuvor beide Partner sich gegenseitig die Kopie ihres Zertifikats, mit dem sie sich ausweisen werden, einander übergeben. Dann installiert A die Kopie des Zertifikats von B bei sich als Gegenstellenzertifikat. Und B installiert die Kopie des Zertifikats von A bei sich als Gegenstellenzertifikat.

⌦ Als Kopie eines Zertifikats auf keinen Fall die PKCS#12-Datei (Dateinamen-Erweiterung *.p12) nehmen und eine Kopie davon der Gegenstelle geben, um eine spätere Kommunikation per X.509-Authentifizierung mit ihr zu ermöglichen! Denn die PKCS#12-Datei enthält auch den privaten Schlüssel, der nicht aus der Hand gegeben werden darf. Siehe „Erstellung von Zertifikaten“ auf Seite 165.

Um eine Kopie eines in den mGuard importierten Maschinenzertifikats zu erstellen, können Sie wie folgt vorgehen:
Auf der Registerkarte Maschinenzertifikate beim betreffenden Maschinenzertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken. (Siehe „Maschinenzertifikate“ auf Seite 169).

CA-Zertifikate

Das von einer Gegenstelle vorgezeigte Zertifikat kann vom mGuard auch anders überprüft werden als durch Heranziehung des lokal auf dem mGuard installierten Gegenstellenzertifikats. Die nachfolgend beschriebene Möglichkeit wird je nach Anwendung statt dessen oder ergänzend verwendet, um gemäß X.509 die Authentizität von möglichen Gegenstellen zu überprüfen: durch das Heranziehen von CA-Zertifikaten.

CA-Zertifikate geben ein Mittel in die Hand, überprüfen zu können, ob das von einer Gegenstelle gezeigte Zertifikat wirklich von der CA signiert ist, die im Zertifikat dieser Gegenstelle angegeben ist.

Ein CA-Zertifikat kann von der betreffenden CA (Certificate Authority) in Dateiform zur Verfügung gestellt werden (Dateinamen-Erweiterung *.cer, *.pem oder *.crt), z. B. frei herunterladbar von der Webseite der betreffenden CA.

Anhand von in den mGuard geladenen CA-Zertifikaten kann der mGuard also überprüfen, ob das "vorgezeigte" Zertifikat einer Gegenstelle vertrauenswürdig ist. Es müssen aber dem mGuard alle CA-Zertifikate verfügbar gemacht werden, um mit dem von der Gegenstelle vorgezeigten Zertifikat eine Kette zu bilden: neben dem CA-Zertifikat der CA, deren Signatur im zu überprüfenden, von der Gegenstelle vorgezeigten Zertifikat steht, auch das CA-Zertifikat der ihr übergeordneten CA usw. bis hin zum Root-Zertifikat. (Siehe im Glossar unter CA-Zertifikat.)

Die Authentifizierung anhand von CA-Zertifikaten macht es möglich, den Kreis möglicher Gegenstellen ohne Verwaltungsaufwand zu erweitern, weil nicht für jede mögliche Gegenstelle deren Gegenstellenzertifikat installiert werden muss.

Erstellung von Zertifikaten

Für die Erstellung eines Zertifikats wird zunächst ein *privater Schlüssel* und der dazu gehörige *öffentliche Schlüssel* benötigt. Zum Erstellen dieser Schlüssel gibt es Programme, mit denen das jeder selbst tun kann. Ein zugehöriges Zertifikat mit dem zugehörigen *öffentlichen Schlüssel* kann man sich ebenfalls selbst erzeugen, wenn ein selbst signiertes Zertifikat entstehen soll. (Hinweise zum Selbstausstellen gibt ein Dokument, welches von der Webseite www.innominate.de aus dem Download-Bereich heruntergeladen werden kann. Es ist als Application Note unter dem Titel "How to obtain X.509 certificates" veröffentlicht.)

Ein zugehöriges von einer CA (Certificate Authority) signiertes Zertifikat muss bei einer CA beantragt werden.

Damit der private Schlüssel zusammen mit dem zugehörigen Zertifikat in den mGuard importiert werden können, müssen diese Bestandteile in eine sogenannte PKCS#12-Datei (Dateinamen-Erweiterung *.p12) eingepackt werden.

Authentifizierungsverfahren

Bei X.509-Authentifizierungen kann der mGuard zwei prinzipiell unterschiedliche Verfahren anwenden.

- Die Authentifizierung einer Gegenstelle erfolgt auf Basis von Zertifikat ⇔ Gegenstellenzertifikat. In diesem Fall muss z. B. bei VPN-Verbindungen für jede einzelne Verbindung angegeben werden, welches Gegenstellenzertifikat herangezogen werden soll.

ODER / UND

- Der mGuard zieht die ihm verfügbar gemachten CA-Zertifikate heran, um zu prüfen, ob das von der Gegenstelle ihm vorgezeigte Zertifikat echt ist. Dazu müssen dem mGuard alle CA-Zertifikate verfügbar gemacht werden, um mit dem von der Gegenstelle vorgezeigten Zertifikat eine Kette zu bilden, bis hin zum Root-Zertifikat.

"Verfügbar machen" bedeutet, dass die betreffenden CA-Zertifikate im mGuard installiert sein müssen (siehe „CA-Zertifikate“ auf Seite 171) und zusätzlich bei der Konfiguration der betreffenden Anwendung (SSH, HTTPS, VPN) referenziert werden müssen.

Ob die beiden Verfahren alternativ oder kombiniert zu verwenden sind, wird bei VPN, SSH und HTTPS unterschiedlich gehandhabt. Siehe dazu die nachfolgenden Tabellen.

SSH: Authentifizierung bei SSH

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert**	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von:	⇕	⇕
	Alle CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellenzertifikate, wenn als Filter verwendet (Siehe „6.2.1 Verwaltung » Systemeinstellungen“ , „Shell-Zugang“ auf Seite 67)	Gegenstellenzertifikat

HTTPS: Authentifizierung bei HTTPS

Die Gegenstelle zeigt vor:	Zertifikat (personenbezogen) von **CA signiert***	Zertifikat (personenbezogen) **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von:	⇕	⇕
	Alle CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigtem Zertifikat die Kette bis zum Root-CA-Zertifikat bilden ggf. PLUS Gegenstellenzertifikate, wenn als Filter verwendet (Siehe „6.2.2 Verwaltung » Web Einstellungen“ , „Zugriff“ auf Seite 75)	Gegenstellenzertifikat

* Die Gegenstelle kann zusätzlich Sub-CA-Zertifikate anbieten. In diesem Fall kann der mGuard mit den angebotenen CA-Zertifikaten und den bei ihm selber konfigurierten CA-Zertifikaten die Vereinigungsmenge bilden, um die Kette zu bilden. Auf jeden Fall muss aber das zugehörige Root-CA-Zertifikat auf dem mGuard zur Verfügung stehen.

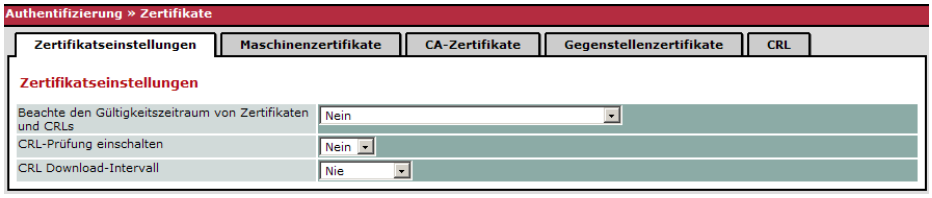
VPN: Authentifizierung bei VPN

Die Gegenstelle zeigt vor:	Maschinenzertifikat von **CA signiert**	Maschinenzertifikat **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von:	⇕	⇕
	Gegenstellenzertifikat ODER Alle CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden	Gegenstellenzertifikat

Wichtig: Es reicht nicht aus, beim mGuard unter *Authentifizierung* » *Zertifikate* die zu verwendenden Zertifikate zu installieren. Zusätzlich muss bei den jeweiligen Anwendungen (VPN, SSH, HTTPS) referenziert werden, welche aus dem Pool der in den mGuard importierten Zertifikate jeweils verwendet werden sollen.

⌦ Das Gegenstellenzertifikat für das Authentifizieren einer VPN-Verbindung (bzw. der Kanäle einer VPN-Verbindung) wird im Menü *IPsec VPN* » *Verbindungen* installiert.

Zertifikats-einstellungen



Zertifikatseinstellungen

Die hier vollzogenen Einstellungen beziehen sich auf alle Zertifikate und Zertifikatsketten, die der mGuard prüfen soll.

Generell ausgenommen davon:

– Selbst signierte Zertifikate von Gegenstellen
– bei VPN alle Gegenstellenzertifikate

Beachte den Gültigkeitszeitraum von Zertifikaten und CRLs: Nein / Warte auf Synchronisation der Systemzeit

Nein: Angaben in Zertifikaten und CRLs über deren Gültigkeitszeitraum werden vom mGuard ignoriert.

Warte auf Synchronisation der Systemzeit

Der in Zertifikaten und CRLs angegebene Gültigkeitszeitraum wird vom mGuard erst dann beachtet, wenn dem mGuard die aktuelle Zeit (Datum und Uhrzeit) bekannt ist, entweder

– durch die eingebaute Uhr (bei *mGuard industrial RS* und *mGuard delta*) oder
– durch Synchronisierung der Systemzeit - siehe „Zeit und Datum“ auf Seite 63.

Bis zu diesem Zeitpunkt werden alle zu prüfenden Zertifikate sicherheitshalber als ungültig erachtet.

CRL-Prüfung einschalten: Ja / Nein

Bei **Ja**: Bei eingeschalteter CRL-Prüfung zieht der mGuard die CRL (Certificate Revocation Liste = Zertifikats-Sperrliste) heran und prüft, ob die dem mGuard vorliegenden Zertifikate gesperrt sind oder nicht.

CRLs werden von den CAs herausgegeben und enthalten die Seriennummern von Zertifikaten, die gesperrt sind, z. B. weil sie als gestohlen gemeldet worden sind.

Auf der Registerkarte **CRL** (siehe „CRL“ auf Seite 175) geben Sie an, von wo der mGuard die Sperrlisten bekommt.

⌦ Bei eingeschalteter CRL-Prüfung ist es notwendig, dass zu jedem *Issuer* von Zertifikaten im mGuard eine CRL konfiguriert sein muss. Fehlende CRLs führen dazu, dass Zertifikate als ungültig betrachtet werden.

⌦ Sperrlisten werden mit Hilfe eines entsprechenden CA-Zertifikats vom mGuard auf Echtheit geprüft. Darum müssen alle zu einer Sperrliste gehörenden CA-Zertifikate (alle Sub-CA-Zertifikate und das Root-Zertifikat) auf dem mGuard importiert sein. Ist die Echtheit einer Sperrliste nicht prüfbar, wird sie vom mGuard so behandelt, als wäre sie nicht vorhanden.

⌦ Ist die Verwendung von Sperrlisten aktiviert und zusätzlich die Beachtung ihrer Gültigkeitszeiträume aktiviert, gelten Sperrlisten als nicht vorhanden, wenn ihre Gültigkeit laut Systemzeit abgelaufen oder noch nicht eingetreten ist.

CRL Download-Intervall

Ist *CRL-Prüfung einschalten* auf **Ja** gesetzt (s. o.), wählen Sie hier aus, nach welchen Zeitabständen die Sperrlisten heruntergeladen und in Kraft gesetzt werden sollen.

Auf der Registerkarte **CRL** (siehe „CRL“ auf Seite 175) geben Sie an, von wo der mGuard die Sperrlisten bekommt.

Ist die CRL-Prüfung eingeschaltet, der CRL-Download aber auf **Nie** gesetzt, muss die CRL manuell in den mGuard geladen worden sein, damit die CRL-Prüfung gelingen kann.

Maschinen-zertifikate

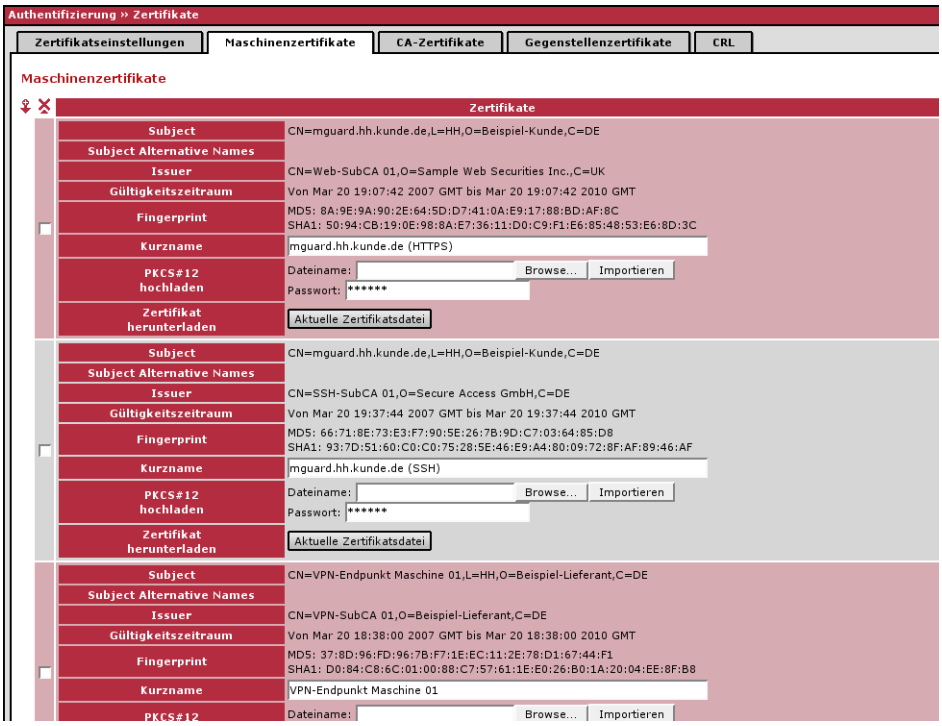
Mit einem Maschinenzertifikat, das in den mGuard geladen ist, authentisiert sich dieser mGuard bei der Gegenstelle. Das Maschinenzertifikat ist sozusagen der Personalausweis eines mGuard, mit dem er sich bei der jeweiligen Gegenstelle ausweist.

Weitere Erläuterungen siehe „Authentifizierung » Zertifikate“ auf Seite 163.

Durch das Importieren einer PKCS#12-Datei erhält der mGuard einen privaten Schlüssel und das dazu gehörige Maschinenzertifikat. Es können mehrere PKCS#12-Dateien in den mGuard geladen werden, so dass der mGuard bei unterschiedlichen Verbindungen jeweils das gewünschte selbst signierte oder von einer CA signierte Maschinenzertifikat verwenden kann, um es der Gegenstelle vorzuzeigen.

⌦ Zur Verwendung eines an dieser Stelle installierten Maschinenzertifikats muss bei der Konfiguration von Anwendungen (SSH, VPN) zusätzlich auf dieses Maschinenzertifikat referenziert werden, um es für die jeweilige Verbindung bzw. die jeweilige Fernzugriffsart zu benutzen.

Beispiel für importierte Maschinenzertifikate:



Maschinenzertifikate

Zeigt die aktuell importierten X.509-Zertifikate an, mit dem sich der mGuard gegenüber Gegenstellen, z. B. anderen VPN-Gateways, ausweist.

Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

Neues Maschinenzertifikat importieren

Voraussetzung:

Die PKCS#12 (Dateiname = *.p12 oder *.pfx) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

1. **Durchsuchen...** klicken, um die Datei zu selektieren
2. In das Feld *Passwort* geben Sie das Passwort ein, mit dem der private Schlüssel der PKCS#12-Datei geschützt ist.
3. **Importieren** klicken.

Nach dem Import ist unter *Zertifikat* das geladene Zertifikat zu sehen. Bitte vergessen Sie nicht, das importierte Zertifikat samt der anderen Eingaben durch einen Klick auf die Schaltfläche **Übernehmen** abzuspeichern.

Kurzname

Beim Importieren eines Maschinenzertifikats wird das CN-Attribut aus dem Subject-Feld des Zertifikats hier als Kurzname vorgeschlagen, sofern das Feld *Kurzname* bis jetzt leer ist. Dieser Name kann übernommen oder frei geändert werden.
Sie müssen einen Namen vergeben, den vorgeschlagenen oder einen anderen. Und Namen müssen eindeutig sein, dürfen also nicht doppelt vergeben werden.

Verwendung des Kurznamens: Bei der Konfiguration
- von SSH (Menü *Verwaltung* » *Systemeinstellungen, Shell-Zugang*),
- von HTTPS (Menü *Verwaltung* » *Web-Einstellungen, Zugriff*) und
- von VPN-Verbindungen (Menü *IPsec VPN* » *Verbindungen*)

werden die in den mGuard importierten Zertifikate per Auswahlliste angeboten. In dieser werden die Zertifikate jeweils unter dem Kurznamen angezeigt, den Sie hier auf dieser Seite den einzelnen Zertifikaten geben. Darum ist eine Namensvergabe zwingend erforderlich.

Zertifikats-Kopie erstellen

Aus dem importierten Maschinenzertifikat können Sie eine Kopie erzeugen. (z. B. für die Gegenstelle, so dass diese den mGuard damit authentifizieren kann). Diese Kopie enthält nicht den privaten Schlüssel und ist deshalb unbedenklich.

Gehen Sie dazu wie folgt vor:

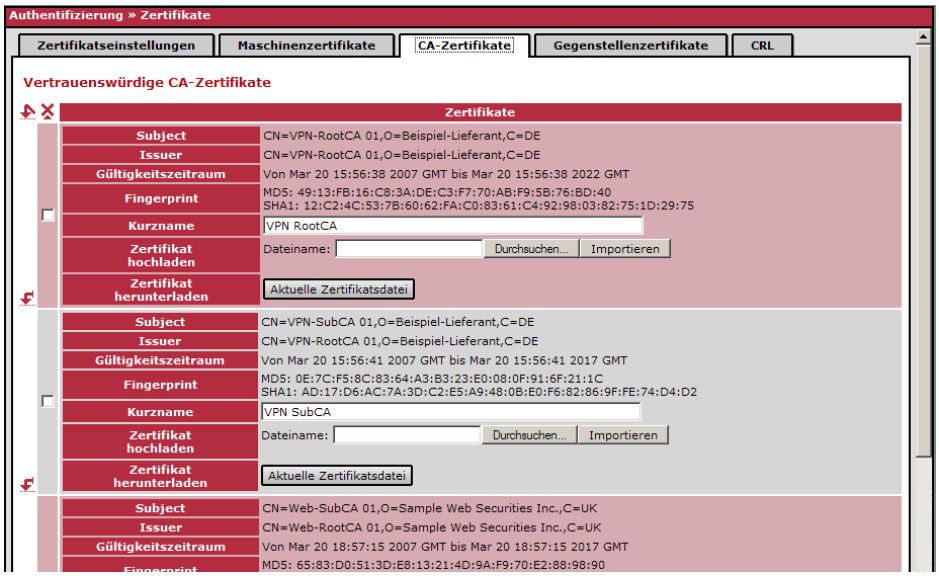
Beim betreffenden Maschinenzertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken. Im sich daraufhin öffnenden Dialogfeld die gewünschten Angaben machen.

CA-Zertifikate

CA-Zertifikate sind Zertifikate von Zertifizierungsstellen (CA). CA-Zertifikate dienen dazu, die von Gegenstellen vorgezeigten Zertifikate auf Echtheit zu überprüfen.

Die Überprüfung geschieht wie folgt: Im von der Gegenstelle übertragenen Zertifikat ist der Zertifikatsaussteller (CA) als Issuer angegeben. Diese Angabe kann mit dem lokal vorliegenden CA-Zertifikat von dem selben Issuer auf Echtheit überprüft werden. Weitere Erläuterungen siehe „Authentifizierung » Zertifikate“ auf Seite 163.

Beispiel für importierte CA-Zertifikate:



Vertauenswürdige CA-Zertifikate

Zeigt die aktuell importierten CA-Zertifikate an.

Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

Neues CA-Zertifikat importieren

Voraussetzung:

Die Datei (Dateinamen-Erweiterung *.cer, *.pem oder *.crt) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

1. **Durchsuchen...** klicken, um die Datei zu selektieren
2. **Importieren** klicken.

Nach dem Import ist unter *Zertifikat* das geladene Zertifikat zu sehen. Bitte vergessen Sie nicht, das importierte Zertifikat samt der anderen Eingaben durch einen Klick auf die Schaltfläche **Übernehmen** abzuspeichern.

Kurzname

Beim Importieren eines CA-Zertifikats wird das CN-Attribut aus dem Subject-Feld des Zertifikats hier als Kurzname vorgeschlagen, sofern das Feld Kurzname bis jetzt leer ist. Dieser Name kann übernommen oder frei geändert werden.

Sie müssen einen Namen vergeben, den vorgeschlagenen oder einen anderen. Und Namen müssen eindeutig sein, dürfen also nicht doppelt vergeben werden.

Verwendung des Kurznamens: Bei der Konfiguration
- von SSH (Menü *Verwaltung* » *Systemeinstellungen, Shell-Zugang*),
- von HTTPS (Menü *Verwaltung* » *Web-Einstellungen, Zugriff*) und
- von VPN-Verbindungen (Menü *IPsec VPN* » *Verbindungen*)

werden die in den mGuard importierten Zertifikate per Auswahlliste angeboten. In dieser werden die Zertifikate jeweils unter dem Kurznamen angezeigt, den Sie hier auf dieser Seite den einzelnen Zertifikaten geben. Eine Namensvergabe ist also zwingend erforderlich.

Zertifikats-Kopie erstellen

Aus dem importierten CA-Zertifikat können Sie eine Kopie erzeugen.

Gehen Sie dazu wie folgt vor:

Beim betreffenden CA-Zertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken. Im sich daraufhin öffnenden Dialogfeld die gewünschten Angaben machen.

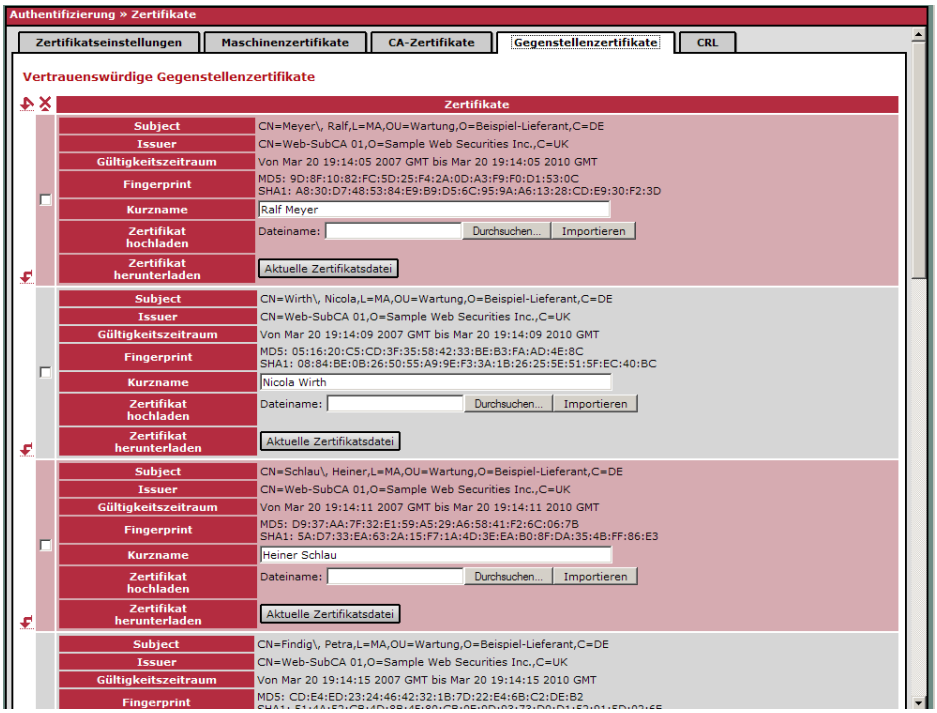
Gegenstellenzertifikate

Ein Gegenstellenzertifikat ist die Kopie des Zertifikats, mit dem sich eine Gegenstelle beim mGuard ausweist. Gegenstellenzertifikate haben Sie von Bedienern möglicher Gegenstellen auf vertrauenswürdigem Wege als Datei (Dateinamen-Erweiterung *.cer, *.pem oder *.crt) erhalten. Diese Datei laden Sie in den mGuard, damit die wechselseitige Authentifizierung gelingen kann. Es können die Gegenstellenzertifikate mehrerer möglicher Gegenstellen geladen werden.

⌦ Das Gegenstellenzertifikat für das Authentifizieren einer VPN-Verbindung (bzw. der Kanäle einer VPN-Verbindung) wird im Menü *IPsec VPN* » *Verbindungen* installiert.

Weitere Erläuterungen siehe „Authentifizierung » Zertifikate“ auf Seite 163.

Beispiel für importierte Gegenstellenzertifikate:



Vertauenswürdige Gegenstellenzertifikate

Zeigt die aktuell importierten Gegenstellenzertifikate an.

Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

Neues Zertifikat importieren

Voraussetzung:

Die Datei (Dateinamen-Erweiterung *.cer, *.pem oder *.crt) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

1. **Durchsuchen...** klicken, um die Datei zu selektieren
2. **Importieren** klicken.

Nach dem Import ist unter *Zertifikat* das geladene Zertifikat zu sehen. Bitte vergessen Sie nicht, das importierte Zertifikat samt der anderen Eingaben durch einen Klick auf die Schaltfläche **Übernehmen** abzuspeichern.

Kurzname

Beim Importieren eines Gegenstellenzertifikats wird das CN-Attribut aus dem Subject-Feld des Zertifikats hier als Kurzname vorgeschlagen, sofern das Feld *Kurzname* bis jetzt leer ist. Dieser Name kann übernommen oder frei geändert werden.

Sie müssen einen Namen vergeben, den vorgeschlagenen oder einen anderen. Und Namen müssen eindeutig sein, dürfen also nicht doppelt vergeben werden.

Verwendung des Kurznamens: Bei der Konfiguration
- von SSH (Menü *Verwaltung » Systemeinstellungen, Shell-Zugang*) und
- von HTTPS (Menü *Verwaltung » Web-Einstellungen, Zugriff*)

werden die in den mGuard importierten Zertifikate per Auswahlliste angeboten. In dieser werden die Zertifikate jeweils unter dem Kurznamen angezeigt,

den Sie hier auf dieser Seite den einzelnen Zertifikaten geben. Eine Namensvergabe ist also zwingend erforderlich.

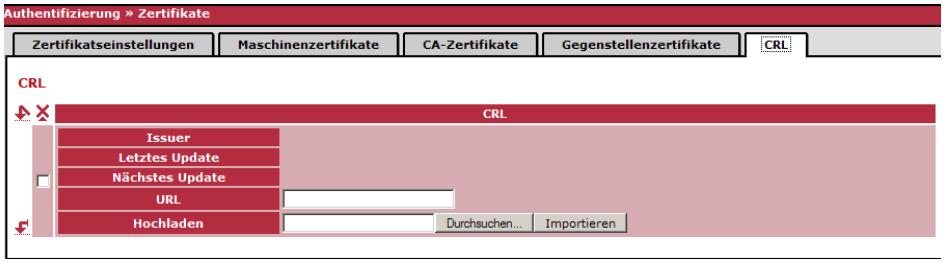
Zertifikats-Kopie erstellen

Aus dem importierten Gegenstellenzertifikat können Sie eine Kopie erzeugen.

Gehen Sie dazu wie folgt vor:

Beim betreffenden Gegenstellenzertifikat neben dem Zeilentitel *Zertifikat herunterladen* auf die Schaltfläche **Aktuelle Zertifikatsdatei** klicken. Im sich daraufhin öffnenden Dialogfeld die gewünschten Angaben machen.

CRL



CRL

CRL - Certificate Revocation List = Zertifikats-Sperrliste.

Die CRL ist eine Liste mit den Seriennummern gesperrter Zertifikate.

Diese Seite dient zur Konfiguration der Stellen, von denen der mGuard CRLs herunterladen soll, um sie verwenden zu können

- Zertifikate werden nur dann auf Sperrung geprüft, wenn auch der Schalter **CRL-Prüfung einschalten** auf **Ja** gesetzt ist. Siehe „Zertifikatseinstellungen“ auf Seite 167.
- Zu jedem Issuer-Namen, der in zu prüfenden Zertifikaten angegeben wird, muss eine CRL mit dem selben Issuer-Namen vorhanden sein. Fehlt eine solche CRL, dann wird bei eingeschalteter CRL-Prüfung das zu prüfende Zertifikat als ungültig betrachtet.

Issuer

Nur Anzeige der Information, die der mGuard direkt aus der CRL liest:

Zeigt den Aussteller der betreffenden Zertifikats-Sperrliste (Certificate Revocation Liste - CRL)

Letztes Update

Nur Anzeige der Information, die der mGuard direkt aus der CRL liest:

Zeit und Datum der Ausstellung der aktuell auf dem mGuard vorhandenen CRL.

Nächstes Update

Nur Anzeige der Information, die der mGuard direkt aus der CRL liest:

Zeit und Datum des Zeitpunktes, zu dem die CA voraussichtlich eine neue CRL veröffentlichen wird.

- Diese Angabe wird weder vom CRL Download-Intervall beeinflusst noch berücksichtigt

URL

Wenn auf der Registerkarte *Zertifikatseinstellungen* (siehe „Zertifikatseinstellungen“ auf Seite 167) unter **CRL Download-Intervall** festgelegt ist, dass die CRL regelmäßig neu heruntergeladen werden soll, dann geben Sie hier die URL der CA an, von der der Download von deren CRL stattfinden kann.

Hochladen

Falls die CRL als Datei vorliegt, kann sie auch manuell in den mGuard geladen werden.

Dazu auf die Schaltfläche **Durchsuchen...** klicken, die Datei selektieren und dann auf **Importieren** klicken. Bitte vergessen Sie nicht, das importierte Zertifikat samt der anderen Eingaben durch einen Klick auf die Schaltfläche **Übernehmen** abzuspeichern.

6.6 Menü Netzwerksicherheit (nicht blade Kontroller)

6.6.1 Netzwerksicherheit » Paketfilter

Der mGuard beinhaltet eine *Stateful Packet Inspection Firewall*. Die Verbindungsdaten einer aktiven Verbindung werden in einer Datenbank erfasst (connection tracking). Dadurch sind Regeln nur für eine Richtung zu definieren. Dann werden die Daten aus der anderen Richtung der jeweiligen Verbindung, und nur diese, automatisch durchgelassen. Ein Nebeneffekt ist, dass bestehende Verbindungen bei einer Umkonfiguration nicht abgebrochen werden, selbst wenn eine entsprechende neue Verbindung nicht mehr aufgebaut werden dürfte.

werkseitige Voreinstellung der Firewall:

- Alle eingehenden Verbindungen werden abgewiesen (außer VPN).
- Die Datenpakete aller ausgehenden Verbindungen werden durchgelassen.

Firewallregeln an dieser Stelle wirken sich aus auf die Firewall, die immer aktiv ist, mit folgenden Ausnahmen:

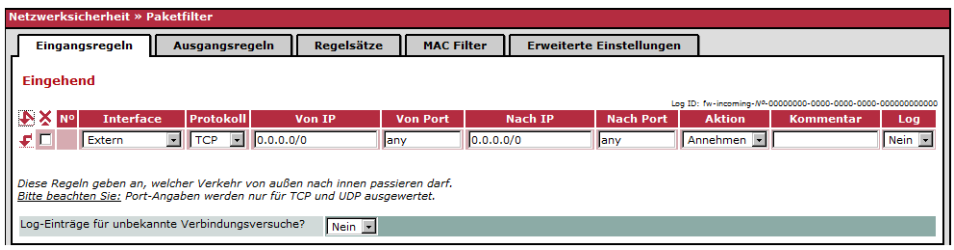
– **VPN-Verbindungen**. Für VPN-Verbindungen werden eigene Firewallregeln definiert - siehe „IPsec VPN » Verbindungen“, „Firewall“ auf Seite 227.

– **Benutzer-Firewall**. Wenn sich Benutzer anmelden, für die Benutzer-Firewall-Regeln definiert sind, werden vorrangig diese Regeln angewandt (siehe „Netzwerksicherheit » Benutzerfirewall“ auf Seite 190), sekundär die immer aktiven Firewall-Regeln.

⌦ Die Anti-Virus-Funktion (siehe „Web-Sicherheit » HTTP“ auf Seite 194, „Web-Sicherheit » FTP“ auf Seite 197, „E-Mail-Sicherheit » POP3“ auf Seite 200, „E-Mail-Sicherheit » SMTP“ auf Seite 203) hat Vorrang vor den hier definierten Firewall-Regeln und kann diese teilweise außer Kraft setzen. Dieses Verhalten kann unter Menü **Netzwerksicherheit** » **Paketfilter**, **Erweiterte Einstellungen** mit dem Schalter **Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln** außer Kraft gesetzt werden - siehe „Erweiterte Einstellungen“, „Anti-Virus Scanner“ auf Seite 185.

⌦ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Eingangsregeln



Eingehend

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert wurden.

Ist keine Regel gesetzt, werden die Datenpakete aller eingehenden Verbindungen (außer VPN) verworfen (= Werkseinstellung).

Bei den Angaben haben Sie folgende Möglichkeiten:

Interface: Extern / Extern 2 / Alle Externen[1]

Gibt an, über welches Interface die Datenpakete eingehen, damit sich die Regel auf sie bezieht. Mit **Alle Externen** sind die Interfaces **Extern** und **Extern 2** gemeint. Diese Interfaces stehen nur bei mGuard-Modellen mit von außen zugänglicher serieller Schnittstelle zur Verfügung.

Protokoll

TCP, UDP, ICMP, Alle.

Von IP / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Von Port / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Namen von Regelsätzen, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen gespeichert sind - siehe Registerkarte *Regelsätze*.

⌧ Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

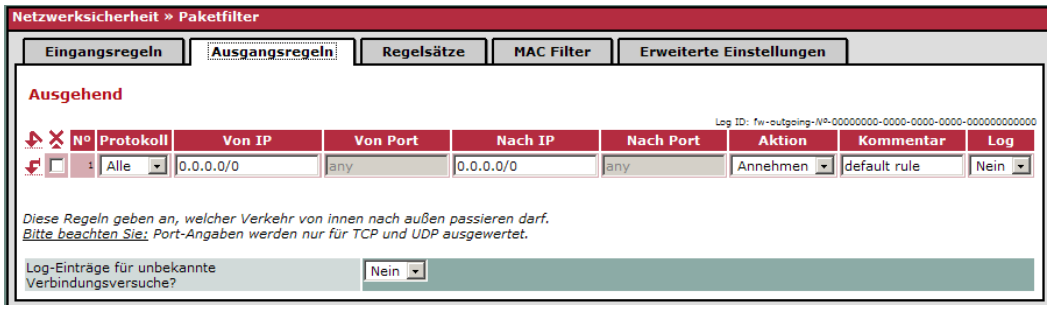
- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche: Ja / Nein

Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werkseitige Voreinstellung: **Nein**)

1. *Extern 2* und *Alle Externen* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

Ausgangsregeln



Ausgehend

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für ausgehende Datenverbindungen, die von intern initiiert wurden, um mit einer entfernten Gegenstelle zu kommunizieren.

Werkseinstellung: Per Werkseinstellung ist eine Regel gesetzt, die alle ausgehenden Verbindungen zulässt.

Ist keine Regel gesetzt, sind alle ausgehenden Verbindungen verboten (außer VPN).

⌧ Die Anti-Virus-Funktion (siehe „Web-Sicherheit » HTTP“ auf Seite 194, „Web-Sicherheit » FTP“ auf Seite 197, „E-Mail-Sicherheit » POP3“ auf Seite 200, „E-Mail-Sicherheit » SMTP“ auf Seite 203) hat Vorrang vor den hier definierten Firewall-Regeln und kann diese teilweise außer Kraft setzen. Dieses Verhalten kann unter Menü **Netzwerksicherheit** » **Paketfilter**, **Erweiterte Einstellungen** mit dem Schalter **Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln** außer Kraft gesetzt werden - siehe „Erweiterte Einstellungen“, „Anti-Virus Scanner“ auf Seite 185.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

TCP, UDP, ICMP, Alle.

Von IP / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Von Port / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Namen von Regelsätzen, sofern definiert. Bei Angabe eines Namens für Regelsätze treten die Firewall-Regeln in Kraft, die unter diesem Namen gespeichert sind - siehe Registerkarte *Regelsätze*.

⌧ Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

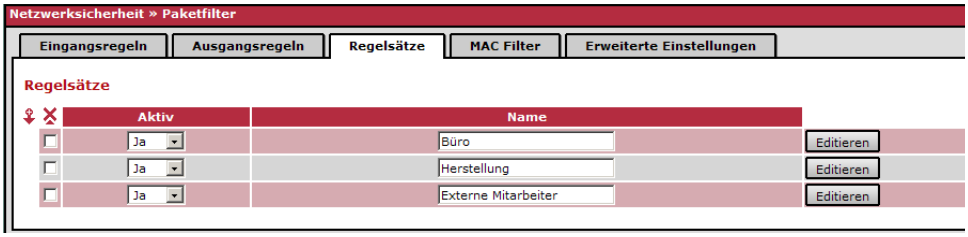
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche: Ja / Nein

Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden. (Werkseitige Voreinstellung: **Nein**)

Regelsätze



Zwecks Strukturierung der Eingangs- und Ausgangsregeln können Sätze von Regeln definiert und jeweils unter einem Namen als Regelsatz abgelegt werden. Dann kann in einer Eingangs- bzw. Ausgangsregel ein Regelsatz referenziert werden, mit dem Effekt, dass die im Regelsatz enthaltenen Regeln dort eingesetzt werden.

Auch ist es möglich, in der Definition eines Regelsatzes selber einen anderen, bereits definierten Regelsatz zu referenzieren, also diesen als Baustein im aktuellen Regelsatz einzusetzen.

Regelsätze

Listet alle Firewall-Regelsätze auf, die definiert worden sind.

Regelsatz neu definieren:

In der Tabelle der Regelsätze rechts im Eintrag mit dem Namen "(unnamed)" auf die Schaltfläche **Editieren** klicken.

Sollte der Eintrag "(unnamed)" nicht sichtbar sein, in der Tabelle der Regelsätze eine weitere Zeile öffnen.

Regelsatz bearbeiten:

Rechts im betreffenden Eintrag auf die Schaltfläche **Editieren** klicken.

⌧ Besteht ein Firewall-Regelsatz aus mehreren Firewall-Regeln, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

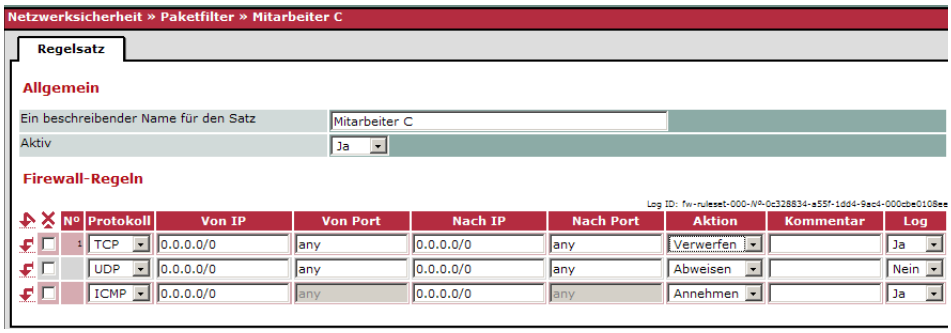
Aktiv: Ja / Nein

Aktiviert / deaktiviert den betreffenden Regelsatz.

Name

Name des Regelsatzes. Der Name ist beim Erstellen des Regelsatzes festgelegt worden.

Nach Klicken auf die Schaltfläche **Editieren** wird die Seite *Regelsatz* angezeigt:



Regelsatz

Allgemein

Ein beschreibender Name für den Satz

Frei zu vergebender Name. Er ist frei wählbar, muss aber einen Regelsatz eindeutig definieren. Über diesen Namen kann ein Regelsatz aus der Liste der Eingangs- und Ausgangsregeln referenziert werden. Dazu wird der betreffende Regelsatz-Name dort in der Spalte *Aktion* ausgewählt.

Aktiv: Ja / Nein

Aktiviert / deaktiviert den betreffenden Regelsatz.

Firewall-Regeln

Protokoll

TCP, UDP, ICMP, Alle.

Von IP / Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Adressenbereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Von Port / Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Namen von Regelsätzen, sofern definiert. Neben "Annehmen", "Abweisen" und "Verwerfen" führt die Auswahlliste auch die Namen bereits definierter Regelsätze auf. Wird ein Name ausgewählt (referenziert), wird dieser, d. h. die Regeln dieses Regelsatzes, an dieser Stelle eingesetzt. Falls die Regeln des eingesetzten Regelsatzes nicht angewendet und mit "Annehmen", "Abweisen" oder "Verwerfen" durchgesetzt werden können, wird mit der Abarbeitung der Regel fortgefahren, die auf die folgt, aus der der Regelsatz referenziert wurde.

⌦ Im Stealth-Modus entspricht **Abweisen** der Aktion **Verwerfen**.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

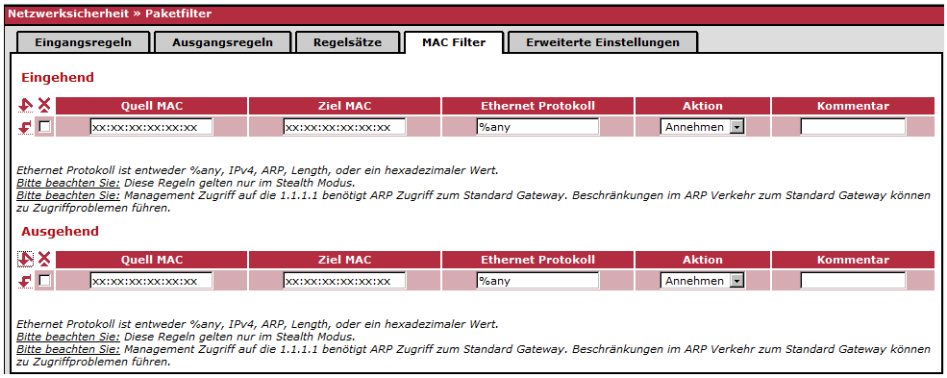
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

⌦ Regelsätze werden nur angewendet, wenn sie auf der Registerkarte *Eingangsregeln* bzw. *Ausgangsregeln* referenziert sind.

⌦ Nur wenn alle Kriterien einer Firewall-Regel erfüllt werden, wird ein Regelsatz, der in dieser Firewall-Regel referenziert wird, angewendet.

MAC Filter


Netzwerksicherheit » Paketfilter
Eingangsregeln
Ausgangsregeln
Regelsätze
MAC Filter
Erweiterte Einstellungen
Eingehend
Quell MAC
Ziel MAC
Ethernet Protokoll
Aktion
Kommentar
xx:xx:xx:xx:xx:xx
xx:xx:xx:xx:xx:xx
%any
Annehmen
Ethernet Protokoll ist entweder %any, IPv4, ARP, Length, oder ein hexadezimaler Wert.
Bitte beachten Sie: Diese Regeln gelten nur im Stealth Modus.
Bitte beachten Sie: Management Zugriff auf die 1.1.1.1 benötigt ARP Zugriff zum Standard Gateway. Beschränkungen im ARP Verkehr zum Standard Gateway können zu Zugriffproblemen führen.
Ausgehend
Quell MAC
Ziel MAC
Ethernet Protokoll
Aktion
Kommentar
xx:xx:xx:xx:xx:xx
xx:xx:xx:xx:xx:xx
%any
Annehmen
Ethernet Protokoll ist entweder %any, IPv4, ARP, Length, oder ein hexadezimaler Wert.
Bitte beachten Sie: Diese Regeln gelten nur im Stealth Modus.
Bitte beachten Sie: Management Zugriff auf die 1.1.1.1 benötigt ARP Zugriff zum Standard Gateway. Beschränkungen im ARP Verkehr zum Standard Gateway können zu Zugriffproblemen führen.

Der MAC Filter wird nur auf Datenpakete angewendet, die über die Ethernet-Schnittstelle eingehen bzw. ausgehen. Datenpakete, die bei mGuard-Modellen mit serieller Schnittstelle[1] per Modemverbindung ein- bzw. ausgehen, werden vom MAC Filter nicht erfasst, weil hier kein Ethernet-Protokoll angewendet wird.

Im *Stealth*-Modus können neben dem Paketfilter (Layer 3/4), der den Datenverkehr z. B. nach ICMP Nachrichten oder TCP/UDP Verbindungen filtert, zusätzlich MAC Filter (Layer 2) gesetzt werden. Ein MAC Filter (Layer 2) filtert nach MAC Adressen und Ethernet Protokollen.

Im Gegensatz zum Paketfilter ist der MAC Filter stateless. Das heißt, werden Regeln eingeführt, müssen gegebenenfalls entsprechende Regeln für die Gegenrichtung ebenfalls erstellt werden.

Ist keine Regel gesetzt, sind alle ARP- und IP-Pakete erlaubt.

- Achten Sie auf die Hinweise auf dem Bildschirm, wenn Sie MAC Filter Regeln setzen.
- Die hier angegebenen Regeln haben Vorrang gegenüber den Packet Filter Regeln.

Quell MAC

Angabe der Quell MAC Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC Adressen.

Ziel MAC

Angabe der Ziel MAC Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC Adressen. Der Wert ff:ff:ff:ff:ff:ff ist die Broadcast MAC Adresse, an die z. B. alle ARP Anfragen geschickt werden.

Ethernet Protokoll

%any steht für alle Ethernet Protokolle. Weitere Protokolle können mit dem Namen oder in HEX angegeben werden, zum Beispiel:

- IPv4 oder 0800
- ARP oder 0806

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren

1. mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta

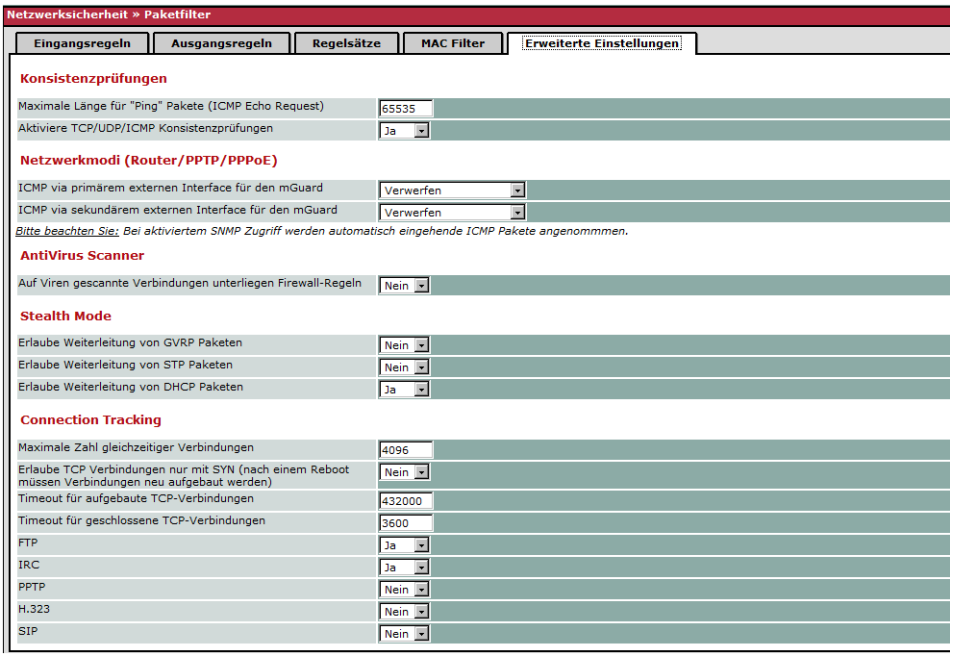
Verwerfen bedeutet, die Datenpakete werden verworfen

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

☞ Der MAC Filter unterstützt keine Logging Funktionalität

Erweiterte Einstellungen



Die Einstellungen betreffen das grundlegende Verhalten der Firewall.

Konsistenzprüfungen

Maximale Länge für "Ping" Pakete (ICMP Echo Request)

Bezieht sich auf die Länge des gesamten Paketes inklusive Header. Normalerweise beträgt die Paketlänge 64 Byte, kann aber auch größer sein. Sollen übergroße Pakete verhindert werden, um "Verstopfungen" zu vermeiden, kann ein maximaler Wert angegeben werden. Dieser sollte auf jeden Fall über 64 liegen, damit normale ICMP Echo Requests nicht blockiert werden.

Aktiviere TCP/UDP/ICMP Konsistenzprüfungen: Ja / Nein

Wenn auf **Ja** gesetzt, führt der mGuard eine Reihe von Tests auf falsche Prüfsummen, Paketgrößen, usw. durch und verwirft Pakete, die die Tests nicht bestehen.

Werkseitig ist dieser Schalter auf **Ja** gesetzt.

Netzwerkmodi (Router / PPTP / PPPoE)

ICMP via primärem externen Interface für den mGuard

ICMP via sekundärem externen Interface für den mGuard

Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Nachrichten beeinflussen, die aus dem externen Netz über das primäre / sekundäre externe Interface an den mGuard gesendet werden. Sie haben folgende Möglichkeiten:

Verwerfen: Alle ICMP-Nachrichten zum mGuard werden verworfen.

Annehmen von Ping: Nur Ping-Nachrichten (ICMP Typ 8) zum mGuard werden akzeptiert.

Alle ICMPs annehmen: Alle Typen von ICMP Nachrichten zum mGuard werden akzeptiert.

⌦ Unabhängig von der hier festgelegten Einstellung werden bei aktiviertem SNMP-Zugriff eingehende ICMP-Pakete immer angenommen.

Anti-Virus Scanner

Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln: Nein / Ja

Unter dem Menü *Web-Sicherheit* » *HTTP, Web-Sicherheit* » *FTP, E-Mail-Sicherheit* » *POP3, E-Mail-Sicherheit* » *SMTP* kann jeweils auf der Registerkarte *Virenschutz* eine Liste von Serververbindungen angelegt werden. Dateien, die über diese Verbindungen beim mGuard eingehen (bei SMTP über den mGuard ausgehen), werden auf Viren gescannt.

Sind Firewall Paketfilter gesetzt (*Netzwerksicherheit* » *Paketfilter* und/oder *Netzwerksicherheit* » *Benutzerfirewall*), die diese Verbindungen betreffen und unterbinden, werden diese nur dann berücksichtigt, sofern der Schalter **Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln** auf **Ja** gesetzt ist. Bei **Nein** (= Standardeinstellung) haben die Regeln, die für die Anti-Virus-Funktion gesetzt sind, Vorrang. Firewall Paketfilter, die dazu im Widerspruch stehen, werden dann außer Kraft gesetzt.

VPN-Verbindungen sind nicht betroffen, weil die Anti-Virus-Funktion bei VPN-Verbindungen nicht zur Verfügung steht.

Stealth-Modus

Erlaube Weiterleitung von GVRP Paketen: Ja / Nein

Das GARP VLAN Registration Protocol (GVRP) wird von GVRP fähigen Switches verwendet, um Konfigurationsinformationen miteinander auszutauschen.

Ist dieser Schalter auf **Ja** gesetzt, dann können GVRP Pakete den mGuard im *Stealth*-Modus passieren.

Erlaube Weiterleitung von STP Paketen: Ja / Nein

Das Spanning-Tree Protocol (STP) (802.1d) wird von Bridges und Switches verwendet, um Schleifen in der Verkabelung zu entdecken und zu berücksichtigen.

Ist dieser Schalter auf **Ja** gesetzt, dann können STP Pakete den mGuard im *Stealth*-Modus passieren.

Erlaube Weiterleitung von DHCP Paketen: Ja / Nein

Bei **Ja** wird dem Client erlaubt, über DHCP eine IP-Adresse zu beziehen - unabhängig von den Firewallregeln für ausgehenden Datenverkehr.

Die Voreinstellung für diesen Schalter ist **Ja**.

Connection Tracking

Maximale Zahl gleichzeitiger Verbindungen

Dieser Eintrag legt eine Obergrenze fest. Diese ist so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht wird. Bei Angriffen kann sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie den Wert erhöhen.

Erlaube TCP-Verbindungen nur mit SYN: Ja / Nein

SYN ist ein spezielles Datenpaket im TCP/IP-Verbindungsaufbau, das den Anfang des Verbindungsaufbaus markiert.

Nein (Standard): Der mGuard erlaubt auch Verbindungen, deren Anfang er nicht registriert hat. D. h. der mGuard kann bei Bestehen einer Verbindung einen Neustart durchführen, ohne dass die Verbindung abreißt.

Ja: Der mGuard muss das SYN-Paket einer bestehenden Verbindung registriert haben. Sonst baut er die Verbindung ab. D. h. falls der mGuard während des Bestehens einer Verbindung einen Neustart durchführt, wird diese Verbindung getrennt. Damit werden Angriffe auf bestehende Verbindungen und das Entführen bestehender Verbindungen erschwert.

Timeout für aufgebaute TCP-Verbindungen

Wird eine TCP Verbindung über den hier angegebenen Zeitraum hinaus nicht verwendet, so werden ihre Verbindungsdaten gelöscht. Eine durch NAT umgeschriebene Verbindung (nicht 1:1-NAT), muss danach erneut aufgebaut werden.
Die Voreinstellung sind 432000 Sekunden (5 Tage).

FTP: Ja / Nein

Wird beim FTP-Protokoll eine ausgehende Verbindung hergestellt, um Daten abzurufen, gibt es zwei Varianten der Datenübertragung: Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. Beim „passiven FTP“ baut der Client diese zusätzliche Verbindung zum Server zur Datenübertragung auf. Damit die zusätzlichen Verbindungen von der Firewall durchgelassen werden, muss **FTP** auf **Ja** stehen (Standard).

IRC: Ja / Nein

Ähnlich wie bei FTP: Beim Chatten im Internet per IRC müssen nach aktivem Verbindungsaufbau auch eingehende Verbindungen zugelassen werden, soll das Chatten reibungslos funktionieren. Damit diese von der Firewall durchgelassen werden, muss **IRC** auf **Ja** stehen (Standard).

PPTP: Ja / Nein

Muss **Ja** gesetzt werden, wenn von lokalen Rechnern ohne Zuhilfenahme des mGuard VPN-Verbindungen mittels PPTP zu externen Rechner aufgebaut werden können sollen.

Werkseitig ist dieser Schalter auf **Nein** gesetzt.

H.323: Ja / Nein

Standard: Nein.

Protokoll, das zum Aufbau von Kommunikationssitzungen mit zwei oder mehr Teilnehmern dient. Wird für audio-visuelle Übertragungen verwendet. Dieses Protokoll ist älter als SIP.

SIP: Ja / Nein

Standard: Nein.

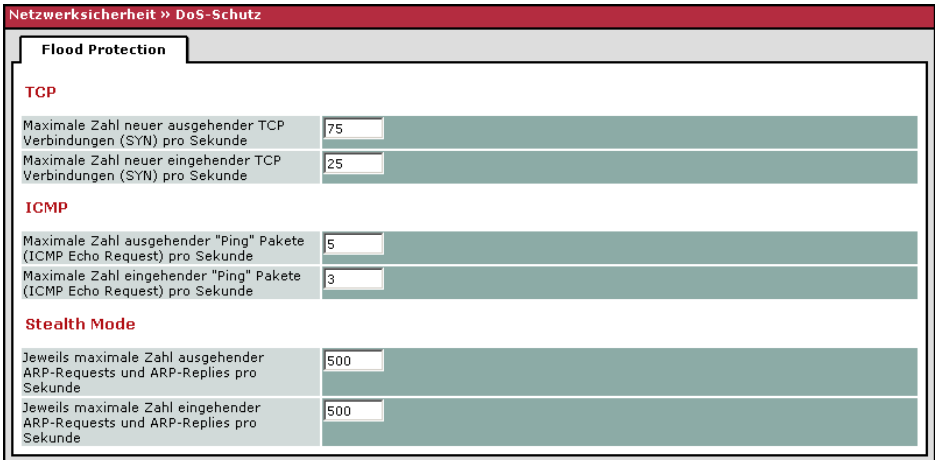
Das SIP (Session Initiation Protocol) dient zum Aufbau von Kommunika-tionssitzungen mit zwei oder mehr Teilnehmern. Wird häufig bei der IP-Telefonie verwendet.

Mit **Ja** ist es dem mGuard möglich, das SIP zu verfolgen und dynamisch notwendige Firewall-Regeln einzufügen, wenn weitere Kommunikationskanäle zu derselben Sitzung aufgebaut werden.

Wenn zusätzlich NAT aktiviert ist, können einer oder mehrere lokal angeschlossene Rechner über den mGuard mit extern erreichbaren Rechnern per SIP kommunizieren.

6.6.2 Netzwerksicherheit » DoS-Schutz

Flood Protection


Netzwerksicherheit » DoS-Schutz
Flood Protection
TCP
Maximale Zahl neuer ausgehender TCP Verbindungen (SYN) pro Sekunde
75
Maximale Zahl neuer eingehender TCP Verbindungen (SYN) pro Sekunde
25
ICMP
Maximale Zahl ausgehender "Ping" Pakete (ICMP Echo Request) pro Sekunde
5
Maximale Zahl eingehender "Ping" Pakete (ICMP Echo Request) pro Sekunde
3
Stealth Mode
Jeweils maximale Zahl ausgehender ARP-Requests und ARP-Replies pro Sekunde
500
Jeweils maximale Zahl eingehender ARP-Requests und ARP-Replies pro Sekunde
500

TCP

Maximale Zahl neuer ausgehender TCP Verbindungen (SYN) pro Sekunde

Werkseinstellung: 75

Maximale Zahl neuer eingehender TCP Verbindungen (SYN) pro Sekunde

Werkseinstellung: 25

Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden TCP-Verbindungen pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

ICMP

Maximale Zahl ausgehender „Ping“ Pakete (ICMP Echo Request) pro Sekunde

Werkseinstellung: 5

Maximale Zahl eingehender „Ping“ Pakete (ICMP Echo Request) pro Sekunde

Werkseinstellung: 3

Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden „Ping“-Pakete pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

☞ Der Wert **0** bewirkt, dass kein „Ping“ Paket durchgelassen bzw. eingelassen wird.

Stealth Mode

Jeweils maximale Zahl ausgehender ARP-Requests und ARP-Replies pro Sekunde

Werkseinstellung: 500

Jeweils maximale Zahl eingehender ARP-Requests und ARP-Replies pro Sekunde

Werkseinstellung: 500

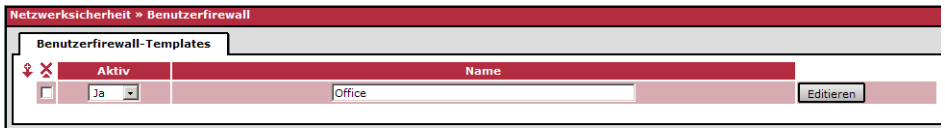
Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden ARP-Requests pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

6.6.3 Netzwerksicherheit » Benutzerfirewall

Die Benutzerfirewall ist ausschließlich bei Firewall-Benutzern in Kraft, also Benutzer, die sich als Firewall-Benutzer angemeldet haben - siehe „Authentifizierung » Firewall-Benutzer“ auf Seite 160. Jedem Firewall-Benutzer kann ein Satz von Firewall-Regeln, ein sogenanntes Template, zugeordnet werden.

⌦ Die Anti-Virus-Funktion (siehe „Web-Sicherheit » HTTP“ auf Seite 194, „Web-Sicherheit » FTP“ auf Seite 197, „E-Mail-Sicherheit » POP3“ auf Seite 200, „E-Mail-Sicherheit » SMTP“ auf Seite 203) hat Vorrang vor den hier definierten Firewall-Regeln und kann diese teilweise außer Kraft setzen. Dieses Verhalten kann unter Menü **Netzwerksicherheit** » **Paketfilter**, **Erweiterte Einstellungen** mit dem Schalter **Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln** außer Kraft gesetzt werden - siehe „Erweiterte Einstellungen“, „Anti-Virus Scanner“ auf Seite 185.

Benutzerfirewall-Templates



Hier werden alle definierten Benutzerfirewall-Templates aufgelistet. Ein Template kann aus mehreren Firewall-Regeln bestehen. Ein Template kann mehreren Nutzern zugeordnet sein.

Template neu definieren:

In der Tabelle der Templates rechts im Eintrag mit dem Namen "(unnamed)" auf die Schaltfläche **Editieren** klicken.

Sollte der Eintrag "(unnamed)" nicht sichtbar sein, in der Tabelle der Regelsätze eine weitere Zeile öffnen.

Regelsatz bearbeiten:

Rechts im betreffenden Eintrag auf die Schaltfläche **Editieren** klicken.

Aktiv: Ja / Nein

Aktiviert / deaktiviert das betreffende Template.

Name

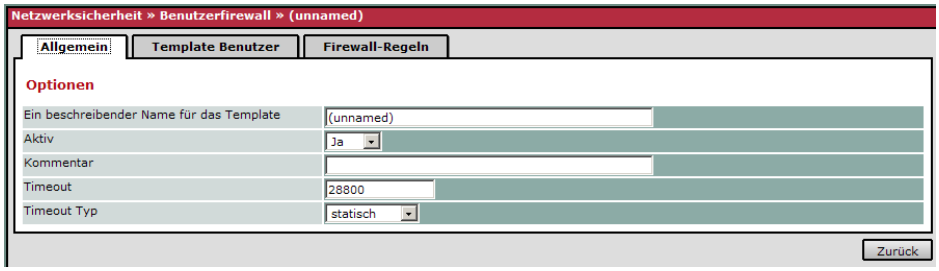
Name des Templates. Der Name ist beim Erstellen des Templates festgelegt worden.

Nach Klicken auf die Schaltfläche **Editieren** wird die Seite *Regelsatz* angezeigt:

Benutzerfirewall » Template editieren

Nach Klicken auf **Editieren** erscheint folgende Registerkarte:

Allgemein



Optionen

Ein beschreibender Name für das Template

Sie können das Benutzerfirewall Template frei benennen bzw. umbenennen.

Aktiv: Ja / Nein

Bei **Ja** ist das Benutzerfirewall-Template aktiv, sobald sich Firewall-Benutzer beim mGuard anmelden, die auf der Registerkarte *Template Benutzer* (s. u.) erfasst sind und denen dieses Template zugeordnet ist. Es spielt keine Rolle, von welchem Rechner und unter welcher IP sich ein Benutzer anmeldet. Die Zuordnung Benutzer - Firewall-Regeln erfolgt über die Authentifizierungsdaten, die der Benutzer bei seiner Anmeldung angibt (Benutzername, Passwort).

Kommentar

Optional: erläuternder Text

Timeout

Standard: 28800.

Gibt in Sekunden an, wann die Firewall-Regeln außer Kraft gesetzt werden. Dauert die Sitzung des betreffenden Benutzers länger als die hier festgelegte Timeout-Zeit, muss er sich neu anmelden.

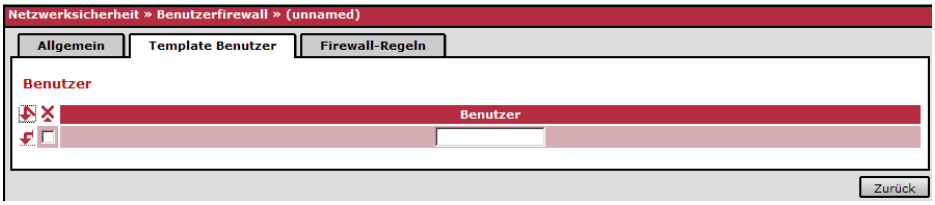
Timeout Typ: statisch / dynamisch

Bei *statischem* Timeout werden Benutzer automatisch abgemeldet, sobald die eingestellte Timeout-Zeit verstrichen ist. Bei *dynamischem* Timeout werden Benutzer automatisch abgemeldet, nachdem die Verbindungen durch den Benutzers geschlossen wurden oder aber auf dem mGuard abgelaufen sind und anschließend die hier eingestellte Timeout-Zeit verstrichen ist.

Eine Verbindung gilt auf dem mGuard dann als abgelaufen, wenn über die folgenden Zeiträume hinaus keine Daten mehr für diese Verbindung vorlagen:

Protokoll	Ablaufzeitraum der Verbindung nach Nichtbenutzung
TCP	5 Tage Dieser Wert ist einstellbar, siehe „Timeout für aufgebaute TCP-Verbindungen“ auf Seite 186. Hinzukommen zusätzliche 120s nach Schließen der Verbindung. (Diese 120s gelten auch nach dem Schließen durch den Benutzer.)
UDP	30s nach Datenverkehr in einer Richtung 180s nach Datenverkehr in beide Richtungen
ICMP	30s
Andere	10min

Template Benutzer

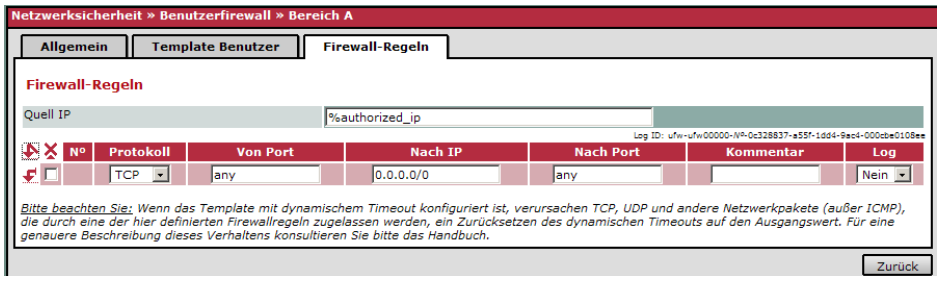


Benutzer

Benutzer

Geben Sie die Namen von Benutzern an. Die Namen müssen denen entsprechen, die unter Menü *Benutzerauthentifizierung* » *Firewall-Benutzer* festgelegt sind - siehe „Authentifizierung » Firewall-Benutzer“ auf Seite 160

Firewall Regeln



Firewall-Regeln

Quell IP

IP Adresse, von der aus Verbindungsaufbauten zugelassen werden. Soll es die Adresse sein, von der sich der Benutzer beim mGuard angemeldet hat, sollte der Platzhalter „%authorized_ip“ verwendet werden.

Sind für einen Benutzer mehrere Firewall-Regeln definiert und aktiviert, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von Port/Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

6.7 Menü Web-Sicherheit (nicht blade Kontroller)

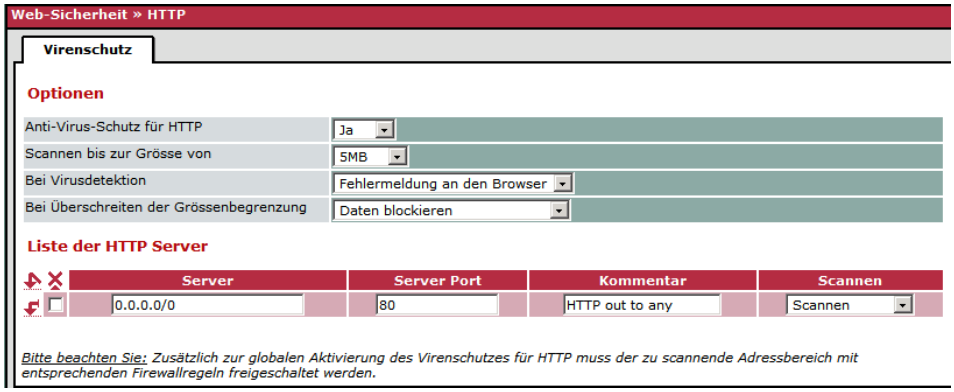
6.7.1 Web-Sicherheit » HTTP

Voraussetzungen:

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Anti-Virus-Lizenz. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt „Verwaltung » Lizenzierung“ auf Seite 82.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt „Verwaltung » Update“ auf Seite 85).

Virenschutz



Das HTTP-Protokoll wird von Web-Browsern zur Übertragung von Webseiten genutzt, hat aber noch viele andere Anwendungen. So wird es z. B. auch zum Download von Dateien wie z. B. Software-Updates oder zur Initialisierung von Multimedia-Streams genutzt.

- Bei aktiviertem Virenschutz erfolgt die Weiterleitung einer übertragenen Datei erst dann, nachdem sie komplett geladen und gescannt wurde. Deshalb kann es bei größeren Dateien oder einer langsamen Download-Geschwindigkeit zu Verzögerungen in der Reaktionszeit der Benutzer-Software kommen.
- Um den Anti-Virus-Schutz für HTTP zu testen, bietet sich zunächst der ungefährliche Eicar-Testvirus an, der eigens für Testzwecke unter der Adresse http://www.eicar.org/anti_virus_test_file.htm heruntergeladen werden kann.
- Der Anti-Virus-Schutz wirkt für HTTP-Verbindungen, die von einem Browser vom lokalen Netzwerk-Interface des mGuards her zum WAN aufgebaut werden. Für in anderen Richtungen aufgebaute Verbindungen wird der Anti-Virus-Schutz nicht angewendet.

Optionen

Anti-Virus-Schutz für HTTP: Ja / Nein

Bei **Ja** werden empfangene und ausgehende Dateien vom mGuard auf Viren gescannt, sofern sie über HTTP-Verbindungen übertragen werden, die unten in der *Liste der HTTP-Server* definiert sind.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an. Dateien, die größer sind, werden nicht gescannt. In diesem Fall wird - abhängig von der Einstellung „bei Überschreiten der Größenbegrenzung“ - eine Fehlermeldung an den Browser gesendet oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software (Browser, Download-Manager) des Benutzers ausgegeben und ein Eintrag im Anti-Virus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlassmodus aktivieren.

Bei Virusdetektion

Fehlermeldung an den Browser

Erkennt der Virenfilter einen Virus innerhalb eines Datentransfers vom HTTP-Server zum HTTP-Client, dann wird eine Fehlermeldung an den HTTP-Client gesendet. Die Darstellung dieser Fehlermeldung hängt vom jeweiligen HTTP-Client ab. Ein Web-Browser wird die Fehlermeldung in Form einer HTML-Seite darstellen. Ist eine innerhalb einer HTML-Seite nachgeladene Datei - z.B. eine Bilddatei - infiziert, so wird diese Datei im Browser nicht angezeigt. Wird ein Dateidownload per HTTP mittels Download-Manager vorgenommen, so wird die Fehlermeldung im Download-Manager angezeigt.

Bei Überschreiten der Grössenbegrenzung

Daten ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall wird nicht auf Viren überprüft!

Daten blockieren

Diese Option bewirkt den Abbruch des Downloads und die Ausgabe eines Fehlercodes an die Client-Software.

Liste der HTTP Server

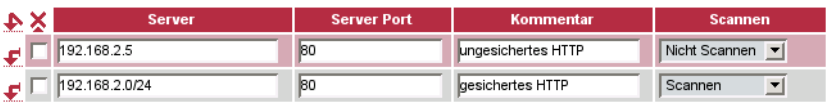
Geben Sie an, von welchen Servern die Daten auf Viren gescannt werden sollen.

Durch Aktivierung bzw. Deaktivierung der Anti-Virus-Funktion bei jedem einzelnen Eintrag bzw. Server haben Sie z. B. die Möglichkeit, eine Ausnahmeregel für eine darauf folgende umfassende Regel zu setzen. Dadurch ist die Angabe von „trusted“ Servern möglich - siehe unten abgebildetes Beispiel.

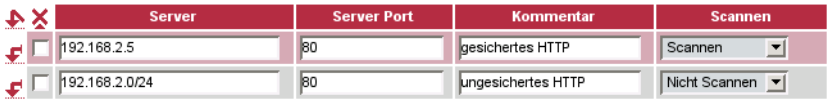
Beispiele:

Globale Aktivierung des Anti-Virus-Schutzes für HTTP:

Scan eines Subnetzes, Ausklammerung eines „trusted“ HTTP-Servers:



Scan eines einzelnen „untrusted“ HTTP-Servers in einem Subnetz:



- Um den Anti-Virus-Schutz für HTTP- bzw. „FTP over HTTP“-Datenverkehr über einen Proxy zu aktivieren, fügen Sie eine neue Zeile in die Liste der Server ein und ersetzen den voreingestellten Port 80 durch den Proxy Port, welcher in Ihrem Web-Browser eingestellt ist.
  Gebräuchliche Proxy-Portnummern sind 3128 und 8080.
- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Nach Viren zu scannen kann ausgehende Verbindungen erlauben, die üblicherweise durch die unter „Netzwerksicherheit » Paketfilter“ und „Netzwerksicherheit » Benutzerfirewall“ definierten Firewallregeln unterbunden sind. Bitte beachten Sie daher auch „Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln: Nein / Ja“ auf Seite 185 um dieses Verhalten anzupassen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. Dateien von allen HTTP-Servern werden gescannt. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

- Da ein Verbindungswunsch zunächst durch den mGuard entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert.

Server Port

Hier geben Sie bitte die Nummer des Ports für das HTTP-Protokoll an. Der HTTP-Standardport **80** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

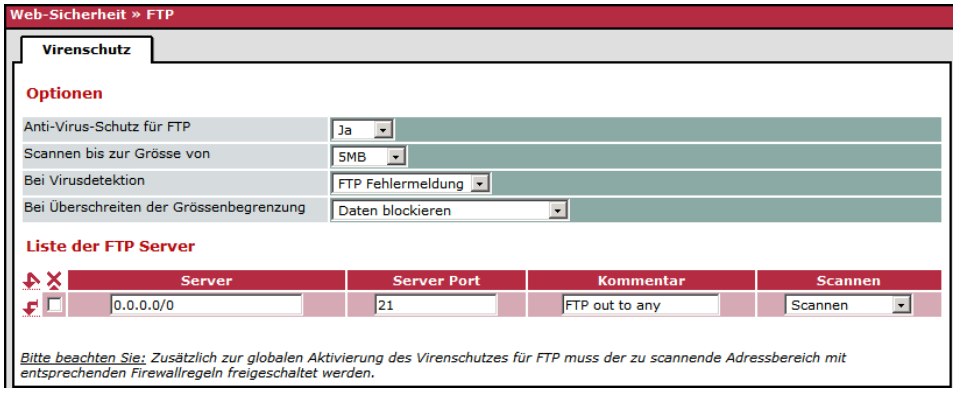
6.7.2 Web-Sicherheit » FTP

Voraussetzungen:

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Anti-Virus-Lizenz. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt „Verwaltung » Lizenzierung“ auf Seite 82.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt „Verwaltung » Update“ auf Seite 85).

Virenschutz



Das FTP-Protokoll wird zum Down- oder Upload von Dateien genutzt.

- Bei aktiviertem Virenschutz erfolgt die Weiterleitung einer übertragenen Datei erst dann, nachdem sie komplett geladen und gescannt wurde. Deshalb kann es bei größeren Dateien oder einer langsamen Download-Geschwindigkeit zu Verzögerungen in der Reaktionszeit der Benutzer-Software kommen.
- Um den Anti-Virus-Schutz für FTP zu testen, bietet sich zunächst der ungefährliche Eicar-Testvirus an, der eigens für Testzwecke unter der Adresse http://www.eicar.org/anti_virus_test_file.htm heruntergeladen werden kann.
- Der mGuard kann nur zum Schutz des FTP-Clients genutzt werden.
- Der Anti-Virus-Schutz wirkt für FTP-Verbindungen, die von einem FTP-Client vom lokalen Netzwerk-Interface des mGuards her zum WAN aufgebaut werden. Für in anderen Richtungen aufgebaute Verbindungen wird der Anti-Virus-Schutz nicht angewendet.

Optionen

Anti-Virus-Schutz für FTP: Ja / Nein

Bei **Ja** werden empfangene und ausgehende Dateien vom mGuard auf Viren gescannt, sofern sie über FTP-Verbindungen übertragen werden, die unten in der *Liste der FTP-Server* definiert sind.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an. Dateien, die größer sind, werden nicht gescannt. In diesem Fall wird - abhängig von der Einstellung „bei Überschreiten der Größenbegrenzung“ - eine Fehlermeldung an den Client gesendet oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software des Benutzers ausgegeben und ein Eintrag im Anti-Virus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download/Upload zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlassmodus aktivieren.

Bei Virusdetektion

FTP Fehlermeldung

Erkennt der Virenfilter einen Virus innerhalb eines Datentransfers zwischen FTP-Server und FTP-Client, dann wird eine Fehlermeldung an den FTP-Client gesendet. Die Darstellung dieser Fehlermeldung hängt vom jeweiligen FTP-Client ab.

Bei Überschreiten der Grössenbegrenzung

Daten ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

⌦ In diesem Fall wird nicht auf Viren überprüft!

Daten blockieren

Diese Option bewirkt den Abbruch des Downloads und die Ausgabe eines Fehlercodes an die Client-Software.

Liste der FTP Server

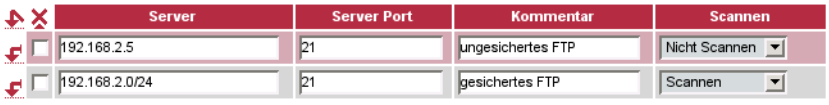
Geben Sie an, von welchen Servern die Daten auf Viren gescannt werden sollen.

Durch Aktivierung bzw. Deaktivierung der Anti-Virus-Funktion bei jedem einzelnen Eintrag bzw. Server haben Sie z. B. die Möglichkeit, eine Ausnahmeregel für eine darauf folgende umfassende Regel zu setzen. Dadurch ist die Angabe von „trusted“ Servern möglich - siehe unten abgebildetes Beispiel.

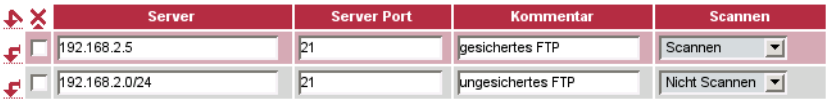
Beispiele:

Globale Aktivierung des Anti-Virus-Schutzes für FTP:

Scan eines Subnetzes, Ausklammerung eines „trusted“ FTP-Servers:



Scan eines einzelnen „untrusted“ FTP-Servers in einem Subnetz:



⌦ Um den Anti-Virus-Schutz für FTP-Datenverkehr über einen Proxy zu aktivieren, fügen Sie eine neue Zeile in die Liste der Server ein und ersetzen den voreingestellten Port 21 durch den Proxy Port.

- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Nach Viren zu scannen kann ausgehende Verbindungen erlauben, die üblicherweise durch die unter „Netzwerksicherheit » Paketfilter“ und „Netzwerksicherheit » Benutzerfirewall“ definierten Firewallregeln unterbunden sind. Bitte beachten Sie daher auch „Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln: Nein / Ja“ auf Seite 185 um dieses Verhalten anzupassen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. Dateien von allen FTP-Servern werden gescannt. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

- Da ein Verbindungswunsch zunächst durch den mGuard entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert.

Server Port

Hier geben Sie bitte die Nummer des Ports für das FTP-Protokoll an. Der FTP-Standardport **21** ist bereits voreingestellt.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

6.8 Menü E-Mail-Sicherheit (nicht blade Kontroller)

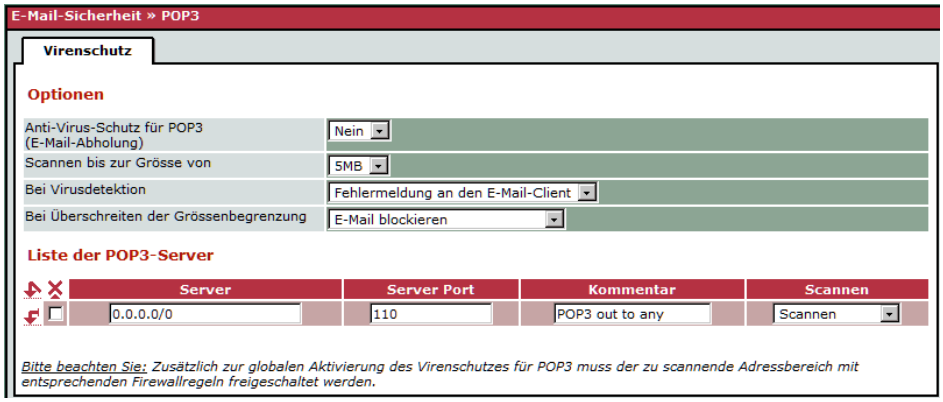
6.8.1 E-Mail-Sicherheit » POP3

Virenschutz

Voraussetzungen:

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Anti-Virus-Lizenz. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt „Verwaltung » Lizenzierung“ auf Seite 82.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt „Verwaltung » Update“ auf Seite 85).



Das POP3-Protokoll wird von Ihrem E-Mail-Client zum Empfang von E-Mails genutzt

- Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie STLS oder SSL nicht aktivieren. Die verschlüsselte Authentifizierung mittels AUTH ist dagegen nutzbar, da die eigentliche Übertragung der E-Mail unverschlüsselt erfolgt.
- Der Anti-Virus-Schutz wirkt für POP3-Verbindungen, die von einem POP3-Client vom lokalen Netzwerk-Interface des mGuards her zum WAN aufgebaut werden. Für in anderen Richtungen aufgebaute Verbindungen wird der Anti-Virus-Schutz nicht angewendet.

Optionen

Anti-Virus-Schutz für POP3 (E-Mail-Abholung): Ja / Nein

Bei **Ja** werden empfangene Dateien vom mGuard auf Viren gescannt, sofern sie über POP3-Verbindungen übertragen werden, die unten in der *Liste der POP3-Server* definiert sind.

⌦ Tipp: Bei einer POP3-Verbindung rufen die meisten E-Mail-Clients alle E-Mails über eine einzige Verbindung ab. Darum kann eine neue Einstellung erst greifen, wenn der E-Mail-Transfer der aktuellen Verbindung vollzogen ist. Falls bei laufendem E-Mail-Transfer die Einstellungen geändert werden sollen, müssen Sie den laufenden Transfer erst abbrechen, damit die neue Einstellung greifen kann.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an. Dateien, die größer sind, werden nicht gescannt. In diesem Fall wird - abhängig von der Einstellung „bei Überschreiten der Größenbegrenzung“ - eine Fehlermeldung an den E-Mail-Client gesendet und die E-Mail nicht empfangen oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an den E-Mail Client des Benutzers ausgegeben und ein Eintrag im Anti-Virus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, das Abholen der E-Mail zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlassmodus aktivieren.

☞ Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Dateigröße sein kann.

Bei Virusdetektion

Benachrichtigung per E-Mail

Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine E-Mail benachrichtigt.

Fehlermeldung an den E-Mail Client

Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine Fehlermeldung an den E-Mail-Client benachrichtigt, wenn er versucht, E-Mail abzuholen.

☞ Ist für die E-Mail-Client-Software die Option „Gelesene E-Mails auf dem Server löschen“ aktiviert, so wird bei der Einstellung „Benachrichtigung per E-Mail“ die infizierte Mail auf dem Server gelöscht, da der E-Mail-Client davon ausgeht, dass die E-Mail erfolgreich übertragen wurde. Ist dies nicht gewünscht (wenn z. B. die infizierte E-Mail auf anderem Weg heruntergeladen werden soll), sollte ausschließlich die Option „Fehlermeldung an den E-Mail Client“ genutzt werden.

bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall findet keine Überprüfung auf Viren statt!

E-Mail blockieren

Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

Liste der POP3 Server

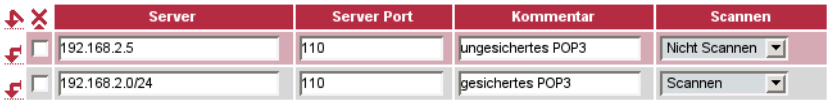
Geben Sie an, von welchen Servern die Daten auf Viren gescannt werden sollen.

Durch Aktivierung bzw. Deaktivierung der Anti-Virus-Funktion bei jedem einzelnen Eintrag bzw. Server haben Sie z. B. die Möglichkeit, eine Ausnahmeregel für eine darauf folgende umfassende Regel zu setzen. Dadurch ist die Angabe von „trusted“ Servern möglich - siehe unten abgebildetes Beispiel.

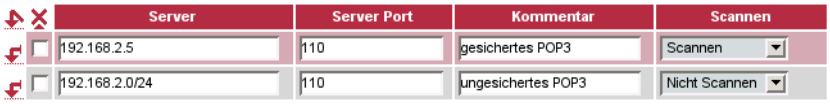
Beispiele:

Globale Aktivierung des Anti-Virus-Schutzes für POP3:

Scan eines Subnetzes, Ausklammerung eines „trusted“ POP3-Servers:



Scan eines einzelnen „untrusted“ POP3 Servers in einem Subnetz:



- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Nach Viren zu scannen kann ausgehende Verbindungen erlauben, die üblicherweise durch die unter „Netzwerksicherheit » Paketfilter“ und „Netzwerksicherheit » Benutzerfirewall“ definierten Firewallregeln unterbunden sind. Bitte beachten Sie daher auch „Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln: Nein / Ja“ auf Seite 185 um dieses Verhalten anzupassen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. Dateien von allen POP3-Servern werden gescannt. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

- Da ein Verbindungswunsch zunächst durch den mGuard entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert.

Server Port

Hier geben Sie bitte die Nummer des Ports für das POP3-Protokoll an. Der POP3-Standardport **110** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

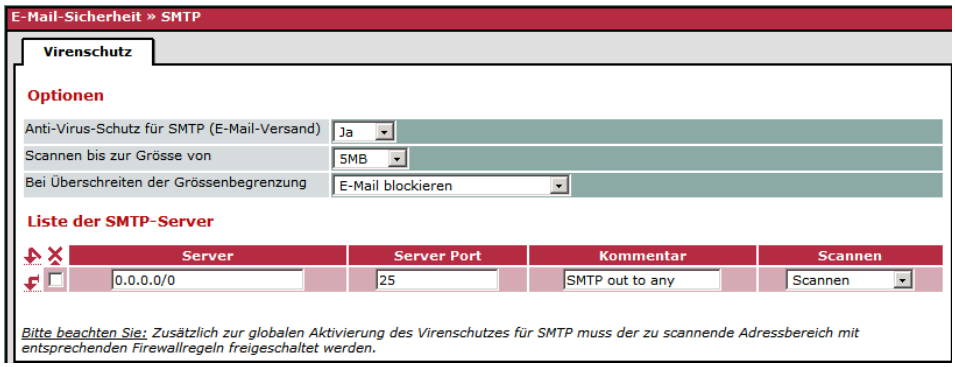
6.8.2 E-Mail-Sicherheit » SMTP

Virenschutz

Voraussetzungen:

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Anti-Virus-Lizenz. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt „Verwaltung » Lizenzierung“ auf Seite 82.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt „Verwaltung » Update“ auf Seite 85).



Das SMTP-Protokoll wird von Ihrem E-Mail-Client oder Mail-Transfer-Agent (MTA) zur Versendung von E-Mails genutzt.

- Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie TLS nicht aktivieren. Im Falle des Erkennens eines Virus oder beim Auftreten von Fehlern wird der E-Mail-Client des Absenders durch einen Fehlercode benachrichtigt und ein Logeintrag im Anti-Virus-Log vorgenommen. Der ursprüngliche Empfänger erhält weder die infizierte Mail noch eine Benachrichtigung.
- Der Anti-Virus-Schutz wirkt für SMTP-Verbindungen, die von einem Mail-Client oder Mail-Server vom lokalen Netzwerk-Interface des mGuards her zum WAN aufgebaut werden. Für in anderen Richtungen aufgebaute Verbindungen wird der Anti-Virus-Schutz nicht angewendet.

Optionen

Anti-Virus-Schutz für SMTP (E-Mail-Versand): Ja / Nein

Bei **Ja** werden ausgehende Dateien vom mGuard auf Viren gescannt, sofern sie über SMTP-Verbindungen übertragen werden, die unten in der *Liste der SMTP-Server* definiert sind.

Scannen bis zur Grösse von

Voreingestellt: 5 MB. Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an. Dateien, die größer sind, werden nicht gescannt. In diesem Fall wird - abhängig von der Einstellung „bei Überschreitung der Grössenbegrenzung“ - eine Fehlermeldung an den SMTP-Client zurückgegeben und die E-Mail nicht gesendet oder automatisch in den Durchlassmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an den E-Mail-Client des Benutzers ausgegeben und ein Eintrag im Anti-Virus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, das Versenden zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig

deaktivieren

- Sie können die Option für den automatischen Durchlassmodus aktivieren.

☞ Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Dateigröße sein kann.

Bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlassmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall wird nicht auf Viren überprüft!

E-Mail blockieren

Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

Liste der SMTP Server

Geben Sie an, bei welchen Servern die Daten auf Viren gescannt werden sollen.

Durch Aktivierung bzw. Deaktivierung der Anti-Virus-Funktion bei jedem einzelnen Eintrag bzw. Server haben Sie z. B. die Möglichkeit, eine Ausnahmeregel für eine darauf folgende umfassende Regel zu setzen. Dadurch ist die Angabe von „trusted“ Servern möglich - siehe unten abgebildetes Beispiel.

Beispiele:

Globale Aktivierung des Anti-Virus-Schutzes für SMTP:

	Server	Server Port	Kommentar	Scannen
	0.0.0.0/0	25	alle ausgehenden Verbindun	Scannen

Scan eines Subnetzes, Ausklammerung eines SMTP-Servers:

	Server	Server Port	Kommentar	Scannen
	192.168.2.5	25	Server mit eigenem AntiVirus	Nicht Scannen
	192.168.2.0/24	25	angreifbare SMTP Server	Scannen

Scan für einen einzelnen SMTP-Server in einem Subnetz:

	Server	Server Port	Kommentar	Scannen
	192.168.2.5	25	angreifbarer SMTP Server	Scannen
	192.168.2.0/24	25	Server mit eigenem AntiVirus	Nicht Scannen

⌦ Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.

⌦ Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.

⌦ Nach Viren zu scannen kann ausgehende Verbindungen erlauben, die üblicherweise durch die unter „Netzwerksicherheit » Paketfilter“ und „Netzwerk-

sicherheit » Benutzerfirewall“ definierten Firewallregeln unterbunden sind. Bitte beachten Sie daher auch „Auf Viren gescannte Verbindungen unterliegen Firewall-Regeln: Nein / Ja“ auf Seite 185 um dieses Verhalten anzupassen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. Dateien zu allen SMTP-Servern werden gescannt. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

⌦ Da ein Verbindungswunsch zunächst durch den mGuard entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert.

Server Port

Hier geben Sie bitte die Nummer des Ports für das SMTP-Protokoll an. Der SMTP-Standardport **25** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

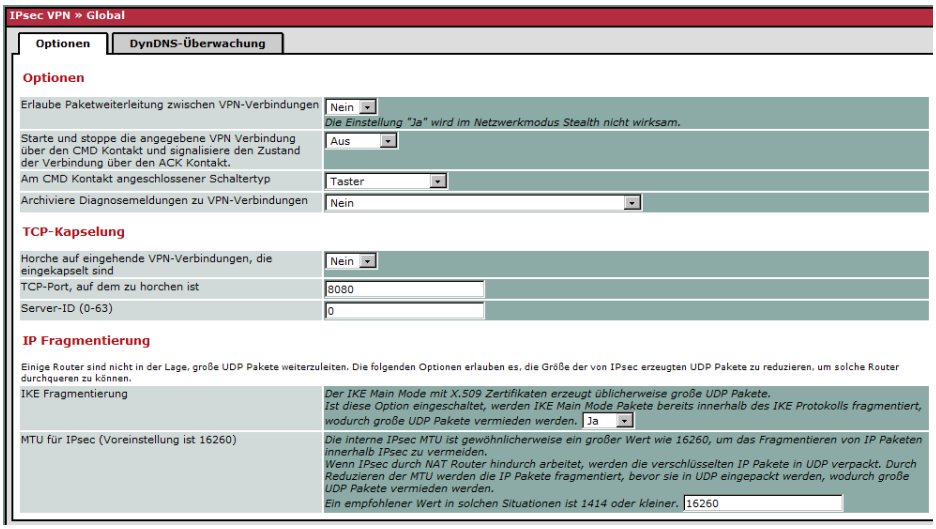
Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

6.9 Menü IPsec VPN (nicht blade Kontroller)

6.9.1 IPsec VPN » Global

Optionen


IPsec VPN » Global
Optionen
DynDNS-Überwachung
Optionen
Erlaube Paketweiterleitung zwischen VPN-Verbindungen
Nein
Die Einstellung "Ja" wird im Netzwerkmodus Stealth nicht wirksam.
Starte und stoppe die angegebene VPN Verbindung über den CMD Kontakt und signalisiere den Zustand der Verbindung über den ACK Kontakt.
Aus
Am CMD Kontakt angeschlossener Schaltertyp
Taster
Archiviere Diagnosemeldungen zu VPN-Verbindungen
Nein
TCP-Kapselung
Horche auf eingehende VPN-Verbindungen, die eingekapselt sind
Nein
TCP-Port, auf dem zu horchen ist
8080
Server-ID (0-63)
0
IP Fragmentierung
Einige Router sind nicht in der Lage, große UDP Pakete weiterzuleiten. Die folgenden Optionen erlauben es, die Größe der von IPsec erzeugten UDP Pakete zu reduzieren, um solche Router durchqueren zu können.
IKE Fragmentierung
Der IKE Main Mode mit X.509 Zertifikaten erzeugt üblicherweise große UDP Pakete.
Ist diese Option eingeschaltet, werden IKE Main Mode Pakete bereits innerhalb des IKE Protokolls fragmentiert, wodurch große UDP Pakete vermieden werden.
Ja
MTU für IPsec (Voreinstellung ist 16260)
Die interne IPsec MTU ist gewöhnlicherweise ein großer Wert wie 16260, um das Fragmentieren von IP Paketen innerhalb IPsec zu vermeiden.
Wenn IPsec durch NAT Router hindurch arbeitet, werden die verschlüsselten IP Pakete in UDP verpackt. Durch Reduzieren der MTU werden die IP Pakete fragmentiert, bevor sie in UDP eingepackt werden, wodurch große UDP Pakete vermieden werden.
Ein empfohlener Wert in solchen Situationen ist 1414 oder kleiner.
16260

Optionen

Erlaube Paketweiterleitung zwischen VPN-Verbindungen: Ja / Nein

Bei **Nein** (Standard): VPN-Verbindungen existieren für sich separat.

Bei **Ja**: Hub and Spoke Feature eingeschaltet: Eine Zentrale unterhält VPN-Verbindungen zu mehreren Zweigstellen, die auch untereinander kommunizieren können.

Bei Aufbau solch einer sternförmigen Topologie von VPN-Verbindungen können Gegenstellen des mGuard auch untereinander Daten austauschen. In diesem Fall ist zu empfehlen, dass der lokale mGuard für die Authentifizierung möglicher Gegenstellen CA-Zertifikate heranzieht - siehe „Authentifizierung“ auf Seite 222.

☞ Die Einstellung **Ja** wird nur auf dem mGuard benötigt, der zwischen zwei verschiedenen VPN-Gegenstellen vermitteln soll.

☞ Damit die Vermittlung zwischen zwei VPN-Gegenstellen funktioniert, muss auf dem vermittelnden mGuard das lokale Netzwerk so konfiguriert werden, dass die Remote-Netze, in denen sich die VPN-Gegenstellen befinden, enthalten sind. Natürlich muss das umgekehrt (lokales und entferntes Netz vertauscht) auch bei den VPN-Gegenstellen so eingerichtet sein. Siehe dazu das Beispiel in der Skizze auf Seite 217.

☞ Die Einstellung **Ja** wird im Netzwerk-Modus *Stealth* nicht unterstützt.

Nur bei mGuard industrial RS

Starte und stoppe die angegebene VPN-Verbindung über den CMD Kontakt...: Aus / *Namen von VPN-Verbindungen*

Der mGuard industrial RS verfügt über Anschlüsse, an die ein externer Taster oder Ein/Aus-Schalter und eine Signal-LED angeschlossen werden können. Über den Taster bzw. Ein/Aus-Schalter kann eine der konfigurierten VPN-Verbindungen aufgebaut und wieder abgebaut werden. Welche VPN-Verbindung das ist, wird hier festgelegt:

Sind unter dem Menüpunkt *IPsec VPN* » *Verbindungen* (siehe „IPsec VPN » Verbindungen“ auf Seite 212) VPN-Verbindungen konfiguriert und aufgelis-

tet, werden diese in der Auswahlliste angezeigt. Soll eine davon manuell auf Tastendruck bzw. durch Schalterbetätigung aufgebaut und wieder abgebaut werden können, wählen Sie diese hier aus.

☞ Ist das Starten und Stoppen der VPN-Verbindung über den CMD-Kontakt eingeschaltet, hat ausschließlich der CMD-Kontakt das Recht dazu. D. h. die Einstellung des Schalters **Aktiv** für die gesamte VPN-Verbindung hat keine Wirkung.
Ist am CMD-Kontakt ein Taster (statt eines Schalters - siehe unten) angeschlossen, kann der Verbindungsaufbau und -abbau aber auch gleichberechtigt und konkurrierend über die Kommandos des CGI-Skriptes nph-vpn.cgi erfolgen.

Bei **Aus** ist diese Funktion ausgeschaltet. Ist an den Service Kontakten des mGuard ein Taster oder Ein/Aus-Schalter angeschlossen, dann hat dessen Betätigung keine Wirkung.

Nur bei mGuard industrial RS

Am CMD Kontakt angeschlossener Schaltertyp: Taster / Ein-/Aus-Schalter

Der mGuard industrial RS verfügt über Anschlüsse, an die ein externer Taster/Schalter und eine Signal-LED angeschlossen werden können. Wählen Sie den Schaltertyp aus, der an den entsprechenden Service-Kontakten des mGuard industrial RS angeschlossen ist.
Mehr dazu siehe „mGuard industrial RS installieren“ auf Seite 24 unter **Service-Kontakte**. Dort wird auch die unterschiedliche Bedienung der Schaltertypen beschrieben.

☞ Ist durch entsprechende Betätigung des Tasters oder Schalters eine VPN-Verbindung aufgebaut, so bleibt diese bestehen, bis sie durch Taster- bzw. Schalterbetätigung wieder abgebaut wird.

☞ Wird ein Ein/Aus-Schalter (statt Taster) verwendet und ist durch dessen Betätigung eine VPN-Verbindung aufgebaut worden, wird diese nach einem Neustart des mGuard automatisch wieder aufgebaut.

Archiviere Diagnosemeldungen zu VPN-Verbindungen: Nein / Nur beim Start mittels nph-vpn.cgi (oder CMD-Kontakt)[1]

Falls beim Aufbau von VPN-Verbindungen Fehler auftreten, kann das Logging des mGuard herangezogen und anhand entsprechender Einträge die Fehlerquelle ausfindig gemacht werden (Siehe Menüpunkt *Logging* » *Logs* ansehen). Diese Möglichkeit zur Fehlerdiagnose ist standardmäßig gegeben, und wenn sie ausreichend ist, setzen Sie diesen Schalter auf **Nein** (Standard).

☞ Damit die Funktion Virenschutz genutzt werden kann, muss die Archivierung von Diagnosemeldungen ausgeschaltet, d. h. auf **Nein** gesetzt sein. Nur dann kann der Virenschutz für HTTP und/oder FTP sowie Virenschutz bei E-Mail für POP3 und/oder SMTP benutzt werden (Menüpunkt *Web-Sicherheit* und Menüpunkt *E-Mail-Sicherheit*).

Option **Nur beim Start mittels nph-vpn.cgi (oder CMD-Kontakt**):

Wird die Möglichkeit zur Diagnose von VPN-Verbindungsproblemen anhand des Loggings des mGuards als zu unpraktisch oder unzureichend empfunden,

1. Der CMD-Kontakt steht nur beim mGuard industrial RS zur Verfügung

wählen Sie diese Option. Das ist möglicherweise der Fall, wenn folgende Bedingungen vorliegen:

– In bestimmten Anwendungsumgebungen, z. B. wenn der mGuard per Maschinensteuerung über den CMD-Kontakt "bedient" wird (nur bei mGuard industrial RS), steht die Möglichkeit, dass ein Anwender über die Web-basierte Bedienoberfläche des mGuard die Logdatei des mGuard einsieht, vielleicht gar nicht zur Verfügung.
– Bei dezentralem Einsatz kann es vorkommen, dass eine Diagnose eines VPN-Verbindungsfehlers erst möglich ist, nachdem der mGuard vorübergehend von seiner Stromquelle getrennt worden ist - was zum Löschen aller Logeinträge führt.
– Die relevanten Logeinträge des mGuard, die Aufschluss geben könnten, sind eventuell gelöscht, weil der mGuard aufgrund seines endlichen Speicherplatzes ältere Logeinträge regelmäßig löscht.
– Wird ein mGuard als zentrale VPN-Gegenstelle eingesetzt, z. B. in einer Fernwartungszentrale als Gateway für die VPN-Verbindungen vieler Maschinen, werden die Meldungen zu Aktivitäten der verschiedenen VPN-Verbindungen im selben Datenstrom protokolliert. Das dadurch entstehende Volumen des Logging macht es zeitaufwendig, die für einen Fehler relevanten Informationen zu finden.

Nach Einschalten der Archivierung werden relevante Logeinträge über die Vorgänge beim Aufbau von VPN-Verbindungen im nicht flüchtigen Speicher des mGuard archiviert, wenn die Verbindungsaufbauten wie folgt veranlasst werden:

– über den CMD-Kontakt

ODER

– über das CGI-Interface nph-vpn.cgi per Kommando "synup" - siehe *Application Note: Diagnosis of VPN connections*. (Application Notes stehen im Download-Bereich von www.innominate.com bereit.)

Archivierte Logeinträge überleben einen Neustart. Sie können als Bestandteil des Support-Snapshots (Menüpunkt *Support* » *Erweitert*, Registerkarte *Snapshot*) heruntergeladen werden. Der Innominate-Support erhält durch solch einen Snapshot erweiterte Möglichkeiten, effizienter nach Problemursachen zu suchen und diese zu finden, als ohne die Archivierung möglich wäre.

Archiviere Diagnosemeldungen nur bei Fehlern: Ja / Nein

Nur sichtbar, wenn Archivierung eingeschaltet ist. Sollen nach Einschalten der Archivierung nur solche Logeinträge archiviert werden, die bei fehlgeschlagenen Verbindungsaufbauversuchen erzeugt werden, setzen Sie diesen Schalter auf **Ja**. Bei **Nein** werden alle Logeinträge archiviert.

☞ Ist die Archivierung von Diagnosemeldungen eingeschaltet, ist es nicht möglich, die Funktion Virenschutz zu nutzen. Das betrifft Virenschutz für HTTP und FTP sowie Virenschutz bei E-Mail für POP3 und SMTP (Menüpunkt *Web-Sicherheit* und Menüpunkt *E-Mail-Sicherheit*).

TCP-Kapselung

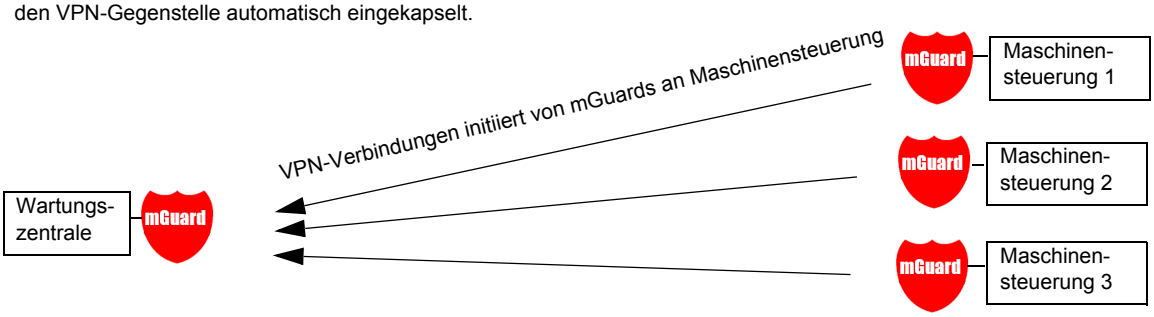
Die Funktion dient dazu, die über eine VPN-Verbindung zu übertragenden Datenpakete in TCP-Pakete einzukapseln. Ohne diese Einkapselung kann es bei VPN-Verbindungen unter Umständen passieren, dass z. B. durch zwischengeschaltete NAT-Router, Firewalls oder Proxy-Server wichtige Datenpakete, die zu einer VPN-Verbindung gehören, nicht ordnungsgemäß übertragen werden. Z. B. können Firewalls so eingestellt sein, dass keine Datenpakete des UDP-Protokolls durchgelassen werden. Oder (mangelhaft implementierte) NAT-Router

könnten bei UDP-Paketen die Port-Nummern nicht korrekt verwalten. Durch die TCP-Kapselung werden diese Probleme vermieden, weil die zur betreffenden VPN-Verbindung gehörenden Pakete in TCP-Pakete eingekapselt, d. h. verborgen sind, so dass für die Netz-Infrastruktur nur TCP-Pakete in Erscheinung treten.

- TCP-Kapselung kann nur eingesetzt werden, wenn auf beiden Seiten des VPN-Tunnels ein mGuard (ab Version 6.1) eingesetzt wird.
- TCP-Kapselung sollte nur eingesetzt werden, wenn es erforderlich ist. Denn durch beträchtliche Vergrößerung des Datenpaket-Overheads und durch entsprechend verlängerte Verarbeitungszeiten werden Verbindungen langsamer.
- Ist beim mGuard unter Menüpunkt *Netzwerk* » *Proxy-Einstellungen* festgelegt, dass ein Proxy für HTTP und HTTPS benutzt wird, dann wird dieser auch für VPN-Verbindungen verwendet, bei denen TCP-Kapselung eingesetzt wird.
- TCP-Kapselung unterstützt die Authentifizierungsverfahren Basic Authentification und NTLM gegenüber dem Proxy.
- Damit die TCP-Kapselung durch einen HTTP Proxy hindurch funktioniert, muss einerseits der Proxy explizit in den Proxy-Einstellungen (Menüpunkt *Netzwerk* » *Proxy-Einstellungen*) benannt werden (also kein transparenter Proxy) und andererseits dieser Proxy die HTTP-Methode CONNECT verstehen und erlauben.

TCP-Kapselung bei einem Anwendungsszenario mit Wartungszentrale und ferngewarteten Maschinen

Als Teilnehmer der TCP-Kapselung initiieren die mGuards der Maschinensteuererungen den VPN-Datenverkehr zur Wartungszentrale und kapseln die zu ihr gesendeten Datenpakete ein. Sobald eine Verbindung initiiert wird, sendet auch die Zentrale die Datenpakete zur betreffenden VPN-Gegenstelle automatisch eingekapselt.



mGuard der Wartungszentrale

Erforderliche Grundeinstellungen
unter Menüpunkt **IPsec VPN,**
Untermenü *Global*,
Register *Optionen*:
Horche auf eingehende VPN-Verbindungen, die eingekapselt sind: **JA**

Untermenü *Verbindungen,*
Register *Allgemein*:
Adresse des VPN Gateways der Gegenstelle: **%any**
Verbindungsinitiierung: **Warte**

mGuards an Maschinensteuererungen

Erforderliche Grundeinstellungen
unter Menüpunkt **IPsec VPN**:
Untermenü *Global,*
Register *Optionen*:
Horche auf eingehende VPN-Verbindungen, die eingekapselt sind: **NEIN**

Untermenü *Verbindungen,*
Register *Allgemein*:
Adresse des VPN Gateways der Gegenstelle: Feste IP-Adresse oder Hostname
Verbindungsinitiierung: **Initiiere** oder **Initiiere bei Datenverkehr**
Kapsele den VPN Datenverkehr in TCP ein: **JA**

Horche auf eingehende VPN-Verbindungen, die eingekapselt sind: Ja / Nein

Standardeinstellung: **Nein**. Nur bei Einsatz der Funktion TCP-Kapselung diesen Schalter auf **Ja** setzen. Nur dann kann der mGuard Verbindungsaufbauten mit eingekapselten Paketen annehmen.

TCP-Port, auf dem zu horchen ist

Nummer des TCP-Ports, über den die zu empfangenen eingekapselten Datenpakete eingehen. Die hier angegebene Portnummer muss mit der Portnummer übereinstimmen, die beim mGuard der Gegenstelle als **TCP-Port des Servers, welche die gekapselte Verbindung annimmt** festgelegt ist (Menüpunkt *IPsec VPN* » *Verbindungen*, Editieren, Registerkarte *Allgemein*).

Es gelten folgende Einschränkungen:

– Der Port, auf dem zu horchen ist, darf nicht identisch sein mit einem Port, der für Fernzugriff benutzt wird (SSH, HTTPS oder SEC-Stick).
– Der Port, auf dem zu horchen ist, darf nicht identisch sein mit einem Port, dessen Verkehr durch die Virenschutzfunktion gefiltertet wird (SMTP, POP3, FTP, HTTP).

Server ID (0-63)

Der Standardwert **0** muss normalerweise nicht geändert werden. Die Nummern dienen zur Unterscheidung unterschiedlicher Zentralen.

Eine andere Nummer muss nur in folgendem Fall verwendet werden: Ein mGuard, vorgeschaltet einer Maschine, muss zu zwei oder mehreren verschiedenen Wartungszentralen und deren mGuards Verbindungen mit eingeschalteter TCP-Kapselung aufnehmen.

IP Fragmentierung

IKE Fragmentierung: Ja / Nein

UDP-Pakete können insbesondere dann übergroß werden, wenn bei Aufbau einer IPsec-Verbindung die Verbindung zwischen den beteiligten Geräten per IKE ausgehandelt wird und dabei Zertifikate ausgetauscht werden. Es gibt Router, die nicht in der Lage sind, große UDP-Pakete weiterzuleiten, wenn diese auf dem Übertragungsweg (z. B. per DSL in 1500 Bytes große Stücke) fragmentiert worden sind. Manches defekte Gerät leitet dann nur das erste Fragment weiter, so dass dann die Verbindung fehlschlägt.

Wenn zwei mGuards miteinander kommunizieren, kann von vornherein dafür gesorgt werden, dass nur kleine UDP-Pakete ausgesandt werden. Damit wird verhindert, dass die Pakete unterwegs fragmentiert und damit möglicherweise von einigen Routern nicht korrekt weitergeleitet werden.

Wenn Sie diese Option nutzen wollen, setzen Sie diesen Schalter auf **Ja**.

⌦ Wird der Schalter auf **Ja** gesetzt, ist diese Einstellung nur wirksam, wenn die Gegenstelle ein mGuard ist, auf dem die Firmware ab Version 5.1.0 installiert ist. In allen anderen Fällen bleibt die Einstellung unwirksam, schadet aber nicht.

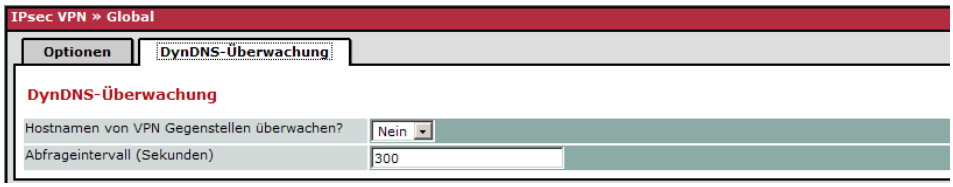
MTU für IPsec (Voreinstellung ist 16260)

Die Option zur Vermeidung übergroßer IKE-Datenpakete, die von defekten Routern auf dem Übertragungsweg nicht korrekt weitergeleitet werden könnten, gibt es auch für IPsec-Datenpakete. Um unter der oft durch DSL ge-

setzten Obergrenze von 1500 Bytes zu bleiben, wird ein Wert von 1414 (Bytes) empfohlen, so dass auch für zusätzliche Header genügend Platz bleibt.

Wenn Sie diese Option nutzen wollen, legen Sie einen niedrigeren Wert als die Voreinstellung fest.

DynDNS-Überwachung



Erläuterung zu DynDNS siehe „ DynDNS“ auf Seite 152.

DynDNS-Überwachung

Hostnamen von VPN Gegenstellen überwachen? Ja / Nein

Ist dem mGuard die Adresse einer VPN-Gegenstelle als Hostname angegeben (siehe „VPN-Verbindung / VPN-Verbindungskanäle definieren“ auf Seite 214), und ist dieser Hostname bei einem DynDNS Service registriert, dann kann der mGuard regelmäßig überprüfen, ob beim betreffenden DynDNS eine Änderung erfolgt ist. Falls ja, wird die VPN-Verbindung zu der neuen IP-Adresse aufgebaut.

Abfrageintervall (Sekunden)

Standard: 300

6.9.2 IPsec VPN » Verbindungen

Voraussetzungen für eine VPN-Verbindung:

Generelle Voraussetzung für eine VPN-Verbindung ist, dass die IP-Adressen der VPN-Partner bekannt und zugänglich sind.

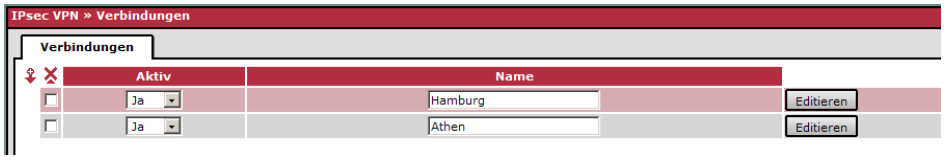
- Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:
  – Authentifizierung über Pre-Shared Key (PSK) oder X.509 Zertifikate
  – ESP
  – Diffie-Hellman Gruppe 2 oder 5
  – DES, 3DES oder AES encryption
  – MD5 oder SHA-1 Hash Algorithmen
  – Tunnel oder Transport Modus
  – Quick Mode
  – Main Mode
  – SA Lifetime (1 Sekunde bis 24 Stunden)
  Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das *Microsoft Windows 2000 High Encryption Pack* oder mindestens das *Service Pack 2* installiert sein.
- Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough). In beiden Fällen sind aus technischen Gründen nur IPsec Tunnel-Verbindungen möglich.

Verbindungen

Liste aller VPN-Verbindungen, die definiert worden sind.

Jeder hier aufgeführte Verbindungsname kann eine einzige VPN-Verbindung oder eine Gruppe von VPN-Verbindungskanälen bezeichnen. Denn es gibt die Möglichkeit, unter den Transport- und/oder Tunneleinstellungen des betreffenden Eintrags mehrere Tunnel zu definieren.

Sie haben die Möglichkeit, neue VPN-Verbindungen zu definieren, VPN-Verbindungen zu aktivieren / deaktivieren, die Eigenschaften einer VPN-Verbindung oder -Verbindungsgruppe zu ändern (editieren) und Verbindungen zu löschen.



VPN-Verbindung / VPN-Verbindungskanäle neu definieren:

In der Tabelle der Verbindungen beim Eintrag mit dem Namen "(unnamed)" auf die Schaltfläche **Editieren** klicken.

Sollte der Eintrag "(unnamed)" nicht sichtbar sein, in der Tabelle eine weitere Zeile öffnen.

VPN-Verbindung / VPN-Verbindungskanäle bearbeiten:

Rechts im betreffenden Eintrag auf die Schaltfläche **Editieren** klicken.

URL für Starten, Stoppen, Statusabfrage einer VPN-Verbindung

Die folgende URL kann verwendet werden, um VPN Verbindungen unabhängig von ihrer **Aktiv** Einstellung zu starten, zu stoppen oder den Verbindungsstatus abzufragen:

`https://`*`server`*`/nph-vpn.cgi?name=`*`verbindung`*`&cmd=(up|down|status)`

Beispiel:

```
wget https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up
```

Ein solches Kommando bezieht sich auf alle Verbindungskanäle, die unter dem betreffenden Namen, in diesem Beispiel *Athen*, zusammengefasst sind. Das ist der Name, der auf der Registerkarte *Allgemein* als "Ein beschreibender Name für die VPN Verbindung" aufgeführt ist. Sofern Mehrdeutigkeit besteht, wirkt der Aufruf des URL nur auf den ersten Eintrag in der Liste der Verbindungen.

Ein Ansprechen einzelner Kanäle einer VPN-Verbindung ist nicht möglich. Sind einzelne Kanäle deaktiviert (**Aktiv**: Nein), werden diese nicht gestartet. Damit hat das Starten und Stoppen auf diesem Wege keine Auswirkung auf die Einstellungen zu den einzelnen Kanälen (= die Liste unter *Transport- und Tunneleinstellungen*).

Das Starten und Stoppen einer Verbindung per URL macht nur Sinn, wenn in der Konfiguration die Verbindung deaktiviert ist (**Aktiv**: Nein) oder wenn die **Verbindungsinitiierung** auf "Warte" eingestellt ist. Ansonsten wird die Verbindung vom mGuard selbständig (wieder) aufgebaut.

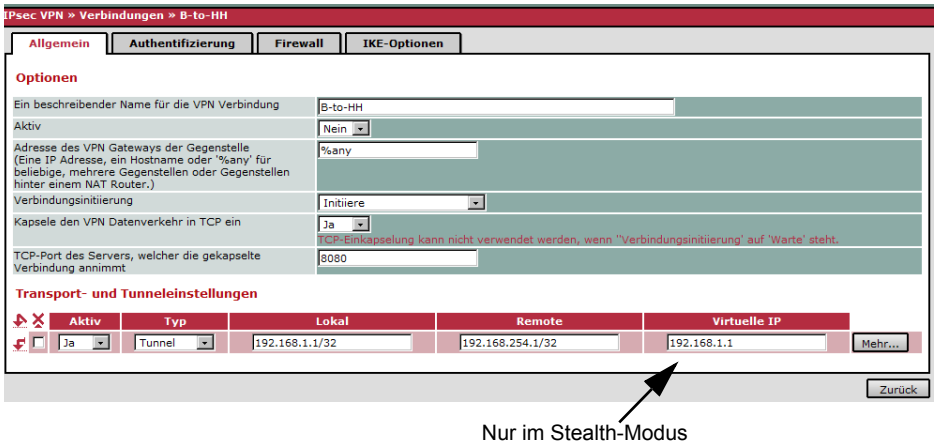
Wird durch Verwendung der oben angegeben URL der Status einer VPN-Verbindung abgefragt, können folgende Antworten erwartet werden:

Antwort	Bedeutung
unknown	Eine VPN-Verbindung mit dem Namen existiert nicht.
void	Die Verbindung ist aufgrund eines Fehlers inaktiv, zum Beispiel weil das externe Netzwerk gestört ist oder weil der Hostname der Gegenstelle nicht in eine IP-Adresse aufgelöst werden konnte (DNS).
ready	Die Verbindung ist bereit, selbst Kanäle aufzubauen oder hereinkommende Anfragen zum Kanalaufbau zu erlauben.
active	Zu der Verbindung ist mindestens ein Kanal auch wirklich aufgebaut.

6.9.3 VPN-Verbindung / VPN-Verbindungskanäle definieren

Nach Klicken auf **Editieren** erscheint je nach Netzwerk-Modus des mGuard (*Stealth*-Modus oder *Router*-Modus u. a. - siehe „Netzwerk » Interfaces“ auf Seite 109) folgende Seite:

Allgemein



Optionen

Ein beschreibender Name für die VPN Verbindung

Sie können die Verbindung frei benennen bzw. umbenennen. Werden weiter unten unter *Transport und Tunneleinstellungen* mehrere Verbindungskanäle definiert, benennt dieser Name das gesamte Set der VPN-Verbindungskanäle, die unter diesem Namen zusammengefasst sind.

Gemeinsamkeiten bei VPN-Verbindungskanälen:

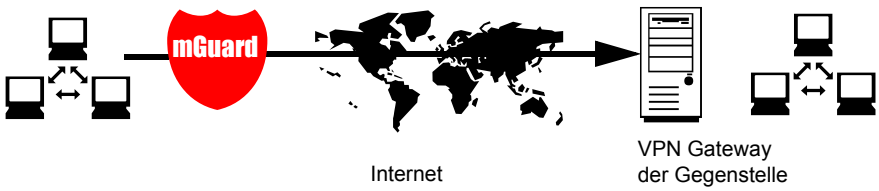
- gleiches Authentifizierungsverfahren, festgelegt auf der Registerkarte *Authentifizierung* (siehe „Authentifizierung“ auf Seite 222)
- gleiche Firewall-Einstellungen
- gleiche Einstellung der IKE-Optionen.

Aktiv: Ja / Nein

Legt fest, ob die unten definierten VPN-Verbindungskanäle insgesamt aktiv (= Ja) sein soll oder nicht (= Nein).

Adresse des VPN Gateways der Gegenstelle

(Eine IP-Adresse, ein Hostname oder **%any** für beliebige, mehrere Gegenstellen oder Gegenstellen hinter einem NAT-Router)



Die Adresse des Übergangs zum privaten Netz, in dem sich der entfernte Kommunikationspartner befindet.

– Falls der mGuard aktiv die Verbindung zur entfernten Gegenstelle initiieren und aufbauen soll, dann geben Sie hier die IP-Adresse oder den Hostnamen der Gegenstellen an.

– Falls das VPN Gateway der Gegenstelle keine feste und bekannte IP-Adresse hat, kann über die Inanspruchname des DynDNS-Service (siehe Glossar) dennoch eine feste und bekannte Adresse simuliert werden.
– Falls der mGuard bereit sein soll, die Verbindung anzunehmen, die eine entfernte Gegenstelle mit beliebiger IP-Adresse aktiv zum lokalen mGuard initiiert und aufbaut, dann geben Sie an: **%any**
Diese Einstellung ist auch bei einer VPN-Sternkonfiguration zu wählen, wenn der mGuard an der Zentrale angeschlossen ist.

So kann eine entfernte Gegenstelle den mGuard „anrufen“, wenn diese Gegenstelle ihre eigene IP-Adresse (vom Internet Service Provider) dynamisch zugewiesen erhält, d. h. eine wechselnde IP-Adresse hat. Nur wenn in diesem Szenario die entfernte „anrufende“ Gegenstelle auch eine feste und bekannte IP-Adresse hat, können Sie diese IP-Adresse angeben.

⌦ **%any** kann nur zusammen mit dem Authentisierungsverfahren über X.509 Zertifikate verwendet werden.

⌦ Wenn die Gegenstelle mit Hilfe von lokal hinterlegten CA-Zertifikaten authentifiziert werden soll, kann die Adresse des VPN Gateway der Gegenstelle konkret (durch IP-Adresse oder Hostname) oder durch **%any** angegeben werden. Wird sie durch eine konkrete Adresse angegeben (und nicht durch "%any"), dann muss ein VPN Identifier (siehe „VPN Identifier“ auf Seite 226) spezifiziert werden.

⌦ Wenn sich die Gegenstelle hinter einem NAT Gateway befindet, muss **%any** gewählt werden. Ansonsten wird das Aushandeln weiterer Verbindungsschlüssel nach der ersten Kontaktaufnahme fehlschlagen.

⌦ Bei Einsatz von **TCP-Kapselung** (siehe „TCP-Kapselung“ auf Seite 208): Es muss eine feste IP-Adresse oder ein Hostname angegeben werden, wenn dieser mGuard die VPN-Verbindung initiieren und den VPN-Datenverkehr einkapseln soll.
Ist dieser mGuard einer Wartungszentrale vorgeschaltet, zu der mehrere entfernte mGuards VPN-Verbindungen herstellen und eingekapselte Datenpakete senden, muss das VPN Gateway der Gegenstelle mit **%any** angegeben werden.

Verbindungsinitiierung: Initiiere / Initiiere bei Datenverkehr / Warte

Initiiere

In diesem Fall initiiert der mGuard die Verbindung zur Gegenstelle. Im Feld *Adresse des VPN Gateways der Gegenstelle* (s. o.) muss die feste IP-Adresse der Gegenstelle oder deren Name eingetragen sein.

Initiiere bei Datenverkehr

Die Verbindung wird automatisch initiiert, wenn der mGuard bemerkt, dass die Verbindung genutzt werden soll.
(Ist bei jeder Betriebsart des mGuard (*Stealth, Router* usw.) wählbar.)

Warte

In diesem Fall ist der mGuard bereit, die Verbindung anzunehmen, die eine entfernte Gegenstelle aktiv zum mGuard initiiert und aufbaut.

☞ Wenn Sie unter *Adresse des VPN Gateways der Gegenstelle* **%any** eingetragen haben, müssen Sie **Warte** auswählen.

Kapsele den VPN Datenverkehr in TCP ein: Nein / Ja

Standard: **Nein**

Bei Anwendung der Funktion **TCP-Kapselung** (siehe „TCP-Kapselung“ auf Seite 208) diesen Schalter nur dann auf **Ja** setzen, wenn der mGuard bei der von ihm initiierten VPN-Verbindung den von ihm ausgehenden Datenverkehr einkapseln soll. In diesem Fall muss auch die Nummer des Ports angegeben werden, über den die Gegenstelle die eingekapselten Datenpakete empfängt.

TCP-Port des Servers, welcher die gekapselte Verbindung annimmt

Standard: **8080**. Nummer des Ports, über den die Gegenstelle die eingekapselten Datenpakete empfängt. Die hier angegebene Portnummer muss mit der Portnummer übereinstimmen, die beim mGuard der Gegenstelle als **TCP-Port, auf dem zu horchen ist** festgelegt ist (Menüpunkt *IPsec VPN* » *Global*, Registerkarte *Optionen*).

⌦ Bei Einsatz von **TCP-Kapselung** (siehe „TCP-Kapselung“ auf Seite 208):

Wenn der mGuard eine VPN-Verbindung zu einer Wartungszentrale aufbauen und den Datenverkehr dorthin einkapseln soll:

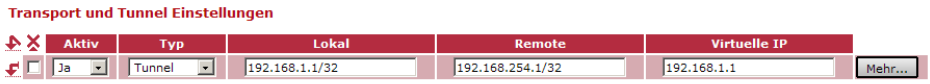
Es muss **Initiiere** oder **Initiiere bei Datenverkehr** festgelegt werden.

Wenn der mGuard bei einer Wartungszentrale installiert ist, zu der mGuards eine VPN-Verbindung aufbauen:

Es muss **Warte** festgelegt werden.

Transport und Tunneleinstellungen

Stealth-Modus:



Hier klicken, wenn weitere Tunnel bzw. Transportwege festgelegt werden sollen.

Router-Modus:

VPN-Verbindungskanäle

Eine unter einem beschreibenden Namen definierte VPN-Verbindung kann aus mehreren VPN-Verbindungskanälen bestehen. Also können Sie hier mehrere VPN-Verbindungskanäle definieren.

Für jeden einzelnen VPN-Verbindungskanal

Nach Klicken auf die Schaltfläche **Mehr...** wird eine weitere Seite zur Festlegung der Verbindungsparameter des betreffenden Transportweges oder Tunnels angezeigt, zum Teil überschneidend.

Aktiv: Ja / Nein

Legen Sie fest, ob der Verbindungskanal aktiv (= Ja) sein soll oder nicht (= Nein).

Kommentar

Frei einzugebender kommentierender Text. Kann leer bleiben.

Typ

Es stehen zur Auswahl:

- Tunnel (Netz ←→ Netz)
- Transport (Host ←→ Host)

Tunnel (Netz ←→ Netz)

Dieser Verbindungstyp eignet sich in jedem Fall und ist der sicherste. In diesem Modus werden die zu übertragenen IP-Datagramme vollkommen verschlüsselt und mit einem neuen Header versehen zum VPN-Gateway der Gegenstelle, dem „Tunnelende“, gesendet. Dort werden die übertragenen Datagramme entschlüsselt und aus ihnen die ursprünglichen Datagramme wiederhergestellt. Diese werden dann zum Zielrechner weitergeleitet.

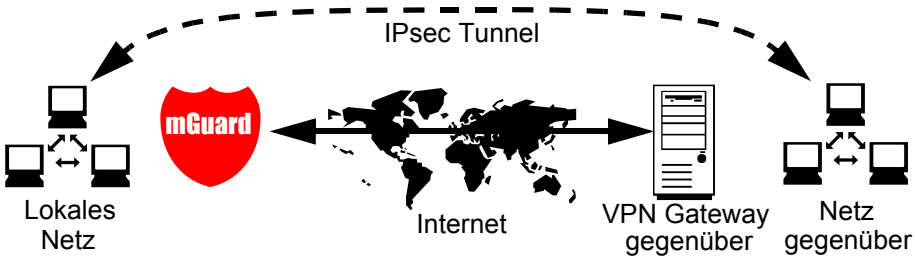
Transport (Host ←→ Host)

Bei diesem Verbindungstyp werden nur die Daten der IP-Pakete verschlüsselt. Die IP Header Informationen bleiben unverschlüsselt.

Bei Wechsel auf *Transport* werden die nachfolgenden Felder (bis auf Protokoll) ausgeblendet, weil diese Parameter entfallen.

Lokal / Remote - bei Verbindungstyp *Tunnel* (Netz ←→ Netz)

Unter **Lokal** und **Remote** definieren Sie die Netzwerkbereiche für beide Tunnelenden.



Lokal

Hier geben Sie die Adresse des Netzes oder Computers an, das oder der lokal am mGuard angeschlossen ist.

Remote

Hier geben Sie die Adresse des Netzes oder Computers an, das/der sich hinter dem gegenüberliegenden VPN Gateway befindet.

Ist oben unter Adresse des *VPN Gateways der Gegenstelle* (siehe „Adresse des VPN Gateways der Gegenstelle“ auf Seite 214) diese mit **%any** angegeben, ist es möglich, dass mehrere verschiedene Gegenstellen zum mGuard Verbindung aufnehmen.

Festlegung einer Default Route über das VPN:

Die Adresse 0.0.0.0/0 gibt eine *Default Route über das VPN* an.
Bei dieser wird sämtlicher Datenverkehr, für den keine anderen Tunnel oder Routen existieren, durch diesen VPN Tunnel geleitet.

⌦ Eine Default Route über das VPN sollte nur für einen einzigen Tunnel angegeben werden.

⌦ Im *Stealth*-Modus kann eine *Default Route über das VPN* nicht verwendet werden.

Option nach Installation einer VPN Tunnel Group Lizenz

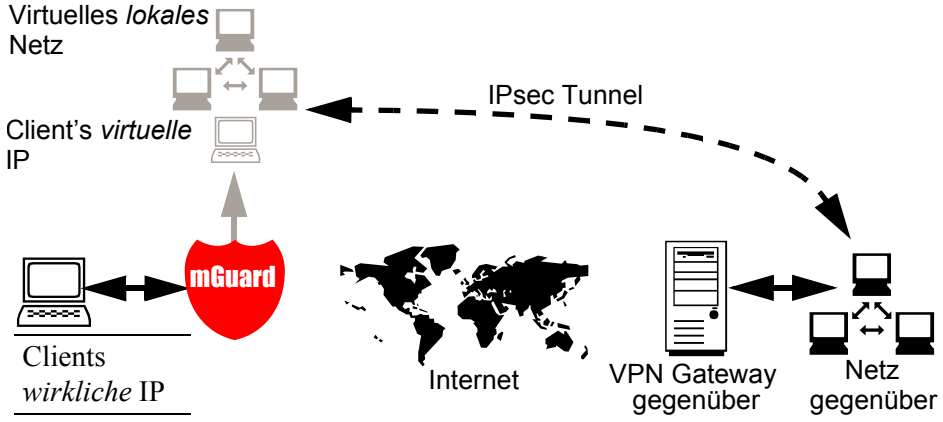
Wird als Adresse des *VPN Gateway der Gegenstelle* **%any** angegeben, können sich auf der entfernten Seite viele mGuards bzw. viele Netzwerke befinden. Dann wird beim lokalen mGuard im Feld **Remote** ein sehr großer Adressenbereich festgelegt, und bei den entfernten mGuards wird jeweils für das bei ihnen unter **Lokal** angegebene Netz ein Teil dieses Adressenbereichs verwendet. Um das zu illustrieren: Die Angaben in den Feldern *Lokal* und *Remote* beim lokalen und bei entfernten mGuards könnten zum Beispiel wie folgt lauten:

Lokaler mGuard			Entfernter mGuard **A**	
Lokal	Remote		Lokal	Remote
10.0.0.0/8	10.0.0.0/8	>	10.1.7.0/24	10.0.0.0/8
			Entfernter mGuard **B**	
			Lokal	Remote
		>	10.3.9.0/24	10.0.0.0/8
			usw.	

Auf diese Weise kann durch die Konfiguration eines einzigen Tunnels der Verbindungsaufbau durch viele Stellen gewährt werden.

⌦ Zur Nutzung dieser Möglichkeiten muss vorher die *VPN Tunnel Group Lizenz* installiert werden, es sei denn, das Gerät wurde bereits entsprechend ausgeliefert. Wird eine solche Lizenz installiert, muss das Gerät erst neu gestartet werden, um sie nutzen zu können.

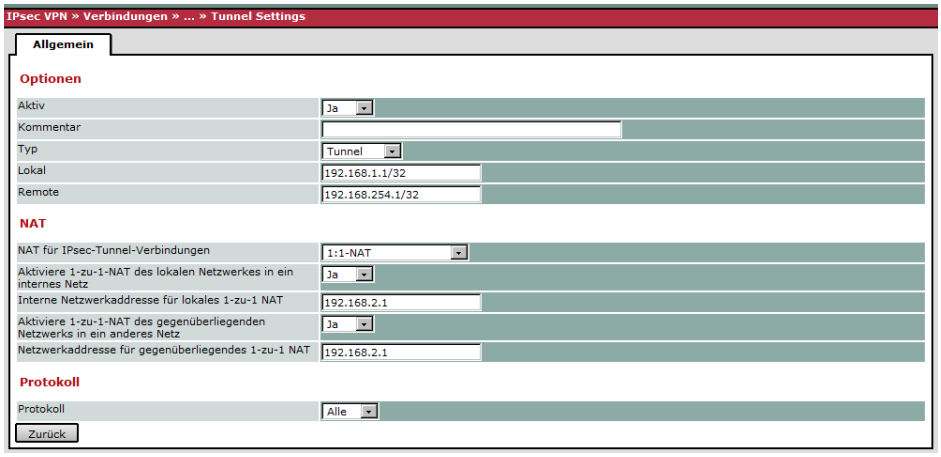
Virtuelle IP *(nur Stealth-Modus)*



Im *Stealth*-Modus wird das lokale Netz des VPNs durch den mGuard simuliert. Innerhalb dieses *virtuellen* Netzes ist der Client unter der hier einzutragenden *virtuellen* IP-Adresse bekannt und ansprechbar.

→ Weitere Einstellungen nach Klicken auf Mehr...

- - Verbindungstyp *Tunnel*



Allgemein

Optionen

Aktiv: Ja / Nein

Wie oben.

Kommentar

Frei einzugebender kommentierender Text. Kann leer bleiben.

Typ: Tunnel / Transport

Wie oben. Bei Wechsel auf *Transport* werden die nachfolgenden Felder (bis auf *Protokoll*) ausgeblendet, weil diese Parameter entfallen.

Lokal

Wie oben.

Remote

Wie oben.

Die virtuelle IP für den Client

Wie oben (vorige Seite).

NAT

NAT für IPsec-Tunnel-Verbindungen: Aus / Lokales Masquerading / 1-zu-1-NAT

Standard: **Aus**

Lokales Masquerading

Kann nur für VPN-Typ *Tunnel* verwendet werden.

Kann im folgenden Fall eingesetzt werden:
Eine Zentrale unterhält zu sehr vielen Zweigstellen jeweils einen VPN-Tunnel. In den Zweigstellen ist jeweils ein lokales Netzwerk mit zahlreichen Rechnern installiert, die über den jeweiligen VPN-Tunnel mit der Zentrale verbunden sind. In diesem Fall könnte der Adressraum zu klein sein, um die Rechner an den verschiedenen VPN-Tunnelenden insgesamt darin unterzubringen. *Lokales Masquerading* schafft hier Abhilfe: Die im Netzwerk einer Zweigstelle angeschlossenen Rechner treten durch das lokale Masquerading für das VPN-Gateway der Zentrale unter einer einzigen IP-Adresse in Erscheinung. Außerdem wird ermöglicht, dass die lokalen Netzwerke in den unterschiedlichen Zweigstel-

len lokal jeweils die selben Netzwerkadresse benutzen. Nur die Zweigstelle kann VPN-Verbindungen zur Zentrale aufbauen.

Interne Netzwerkadresse für lokales Masquerading

Gibt das Netz, d. h. den IP-Adressenbereich an, für den das lokale Masquerading angewendet wird. Nur wenn ein Rechner eine IP-Adresse aus diesem Bereich hat, wird in den Datenpaketen, die dieser Rechner über die VPN-Verbindung aussendet, die Absenderadresse gegen die ausgetauscht, die im Feld **Lokal** angegeben ist (siehe oben).

Die im Feld **Lokal** angegebene Adresse muss die Netzmaske /32 haben, damit es sich um genau eine IP-Adresse handelt.

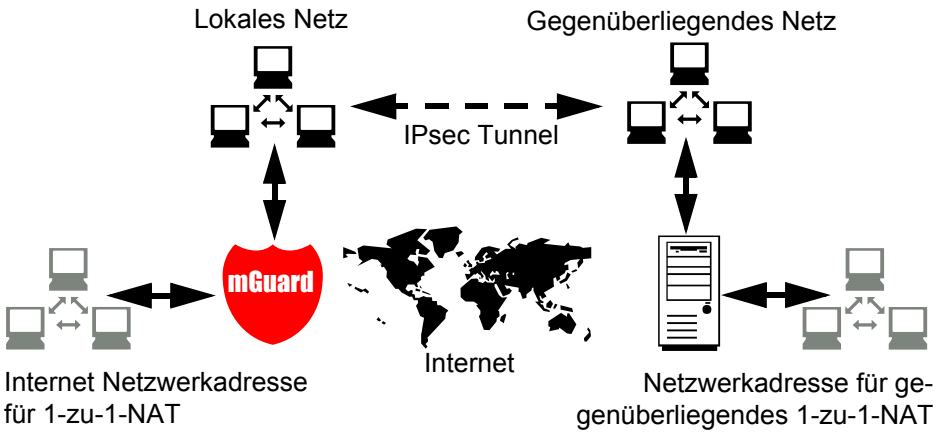
☞ Lokales Masquerading kann in folgenden Netzwerkmodi verwendet werden: Router, PPPoE, PPTP, Modem, Eingebautes Modem und Stealth (nur Stealth-Modus „mehrere Clients“)[1].

☞ Für IP-Verbindungen, die durch eine VPN-Verbindung mit aktiviertem lokalem Masquerading vermittelt werden, werden die Firewall-Regeln für ausgehende Daten in der VPN-Verbindung auf die originale Quelladresse der Verbindung angewendet.

1-zu-1-NAT

Nur im Router-Modus

Mit Hilfe von 1-zu-1-NAT im VPN können weiterhin die tatsächlich genutzten Netzwerkadressen - lokal und/oder entfernt - zur Angabe des Tunnelanfangs bzw. -endes angegeben werden, unabhängig von den mit der Gegenseite vereinbarten Tunnelparametern:



Aktiviere 1-zu-1-NAT des lokalen Netzwerkes in ein internes Netz: Ja / Nein

Das unter *Lokal* angegebene lokale Netzwerk auf ein tatsächlich vorhandenes lokales Netzwerk umschreiben.
Die Voreinstellung ist **Nein**.

Interne Netzwerkadresse für lokales 1-zu-1-NAT

(nur wenn oben **Ja** gewählt wurde)

Die tatsächliche Netzwerkadresse der Systeme im lokalen Netz.
Die Netzmaske wird aus dem Feld **Lokal** übernommen.

1. **Modem / Eingebautes Modem*: Steht nicht bei allen mGuard-Modellen zur Verfügung - siehe „Netzwerk » Interfaces“ auf Seite 109.

Aktiviere 1-zu-1-NAT des gegenüberliegenden Netzwerks in ein anderes Netz

Das unter *Remote* mit der VPN Gegenstelle vereinbarte gegenüberliegende Netzwerk so umschreiben, als wenn sich die dort angeschlossenen Rechner mit deren Adressen in einem anderen Netz befänden.

Die Voreinstellung ist **Nein**.

Netzwerkadresse für gegenüberliegendes 1-zu-1-NAT

(nur wenn oben **Ja** gewählt wurde)

Die von den Systemen im lokalen Netz tatsächlich erreichbare gegenüberliegende Netzwerkadresse.
Die Netzmaske wird aus dem Feld *Remote* übernommen.

⌦ Wenn das *gegenüberliegende Netzwerk* bzw. das *gegenüberliegende Netzwerk für 1-zu-1-NAT* innerhalb eines der direkt am LAN-Port des mGuard angeschlossenen Netzwerke liegt, so beantwortet der mGuard zusätzlich ARP Anfragen für IP Adressen innerhalb des gegenüberliegenden Netzwerks. Damit wird der Zugriff auf ein gegenüberliegendes VPN über lokale IP Adressen möglich, ohne dass das Routing lokal angeschlossener Clients ergänzt werden muss.

Protokoll

Protokoll: Alle / TCP / UDP / ICMP

Sie können auswählen, ob das VPN auf ein bestimmtes Protokoll eingeschränkt werden soll oder aber für den gesamten Datenverkehr gilt.

Bei Auswahl von TCP oder UDP:

Protokoll
TCP
Lokaler Port
('%all' für alle Ports, eine Nummer zwischen 1 und 65535 oder '%any' um den Vorschlag dem Client zu überlassen.)
%all
Remote-Port
('%all' für alle Ports oder eine Nummer zwischen 1 und 65535.)
%all

Lokaler Port

Mit **%all** (Standard) wird festgelegt, dass alle Ports benutzt werden können. Soll ein bestimmer Port verwendet werden, geben Sie dessen Nummer an. Mit **%any** legen Sie fest, dass die Auswahl des Ports dem Client überlassen ist.

Remote-Port

Mit **%all** (Standard) wird festgelegt, dass alle Ports benutzt werden können. Soll ein bestimmer Port verwendet werden, geben Sie dessen Nummer an.

Einstellung für Tunneleinstellung IPsec / L2TP

Wenn sich Clients per IPsec/L2TP über den mGuard verbinden sollen, dann aktivieren Sie den L2TP Server und machen in den nachfolgend aufgelisteten Feldern die jeweils dahinter stehenden Angaben:

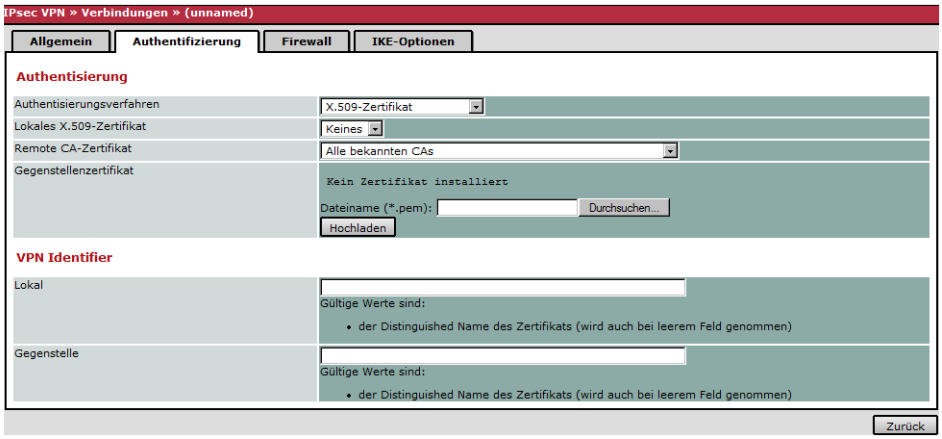
Typ: Transport

Protokoll: UDP

Lokaler Port: %all

Remote-Port: %all

Authentifizierung



Authentisierung

Authentisierungsverfahren

Es gibt 2 Möglichkeiten:

– X.509 Zertifikat (Standard)
– Pre-Shared Key

Je nach dem, welches Verfahren Sie auswählen, zeigt die Seite unterschiedliche Einstellmöglichkeiten.

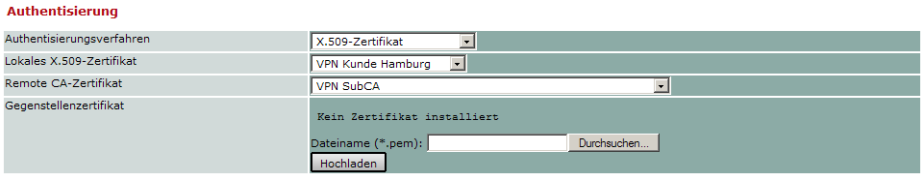
➔ Bei Authentisierungsverfahren X.509 Zertifikat

Dieses Verfahren wird von den meisten neueren IPsec-Implementierungen unterstützt. (Dabei besitzt jeder VPN Teilnehmer einen privaten geheimen Schlüssel sowie einen öffentlichen Schlüssel in Form eines X.509 Zertifikats, welches weitere Informationen über seinen Eigentümer und einer Beglaubigungsstelle (Certification Autority, CA) enthält.)

Es muss Folgendes festgelegt werden:

a) Wie sich der mGuard bei der Gegenstelle authentisiert.

b) Wie der mGuard die entfernte Gegenstelle authentifiziert.



➔ a) ....wie sich der mGuard bei der Gegenstelle authentisiert

Lokales X.509-Zertifikat

Legt fest, mit welchem Maschinenzertifikat sich der mGuard bei der VPN-Gegenstelle ausweist.

In der Auswahlliste eines der Maschinenzertifikate auswählen.

Die Auswahlliste stellt die Maschinenzertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen worden sind - siehe in diesem Handbuch unter „Authentifizierung » Zertifikate“ auf Seite 163.

☞ Falls nur der Eintrag ***Keines*** zu sehen ist, muss erst ein Zertifikat installiert werden. Der Eintrag ***Keines*** darf nicht belassen werden, weil sonst keine X.509-Authentisierung möglich ist.

→ a) ....wie der mGuard die entfernte Gegenstelle authentifiziert

Nachfolgend wird festgelegt, wie der mGuard die Authentizität der entfernten VPN-Gegenstelle prüft.

Die Tabelle unten zeigt, welche Zertifikate dem mGuard zur Authentifizierung der VPN-Gegenstelle zur Verfügung stehen müssen, wenn die VPN-Gegenstelle bei Verbindungsaufnahme eines der folgenden Zertifikatstypen vorzeigt:

- ein von einer CA signiertes Maschinenzertifikat
- ein selbst signiertes Maschinenzertifikat

Zum Verständnis der nachfolgenden Tabelle siehe Kapitel „6.5.3 Authentifizierung » Zertifikate“ auf Seite 163.

Authentifizierung bei VPN

Die Gegenstelle zeigt vor:	Maschinenzertifikat von **CA signiert**	Maschinenzertifikat **selbst signiert**
Der mGuard authentifiziert die Gegenstelle anhand von:	⇳	⇳
	Gegenstellenzertifikat ODER Alle CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden	Gegenstellenzertifikat

Gemäß dieser Tabelle sind nachfolgend dem mGuard die Zertifikate zur Verfügung zu stellen, die er zur Authentifizierung der jeweiligen VPN-Gegenstelle heranziehen muss.

Die nachfolgenden Anleitungen gehen davon aus, dass die Zertifikate bereits ordnungsgemäß im mGuard installiert sind. Siehe „6.5.3 Authentifizierung » Zertifikate“ auf Seite 163 (abgesehen vom Gegenstellenzertifikat - s. u.).

⌧ Ist unter Menüpunkt *Authentifizierung » Zertifikate, Zertifikatseinstellungen* die Verwendung von Sperrlisten (= CRL-Prüfung) aktiviert, wird jedes von einer CA signierte Zertifikat, das VPN-Gegenstellen "vorzeigen", auf Sperrung geprüft. Ausgenommen sind lokal konfigurierte (hier importierte) Gegenstellenzertifikate.

Remote CA-Zertifikat

➧ Wenn sich die VPN-Gegenstelle mit einem **selbst signierten** Maschinenzertifikat authentisiert:

In diesem Fall wählen Sie aus:

Kein CA-Zertifikat, sondern das Gegenstellenzertifikat unten

Dann ist unten unter *Gegenstellenzertifikat* das Gegenstellenzertifikat zu installieren.

☞ Es ist nicht möglich, ein Gegenstellenzertifikat zu referenzieren, das unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen ist.

➨ Wenn sich die VPN-Gegenstelle mit einem **von einer CA signierten** Maschinenzertifikat authentisiert:

Es gibt die Möglichkeit, das von der Gegenstelle vorgezeigte Maschinenzertifikat wie folgt zu authentifizieren;

A durch CA-Zertifikate
B durch das entsprechende Gegenstellenzertifikat

A Authentifizierung durch CA-Zertifikate:

An dieser Stelle ist ausschließlich das CA-Zertifikat von der CA zu referenzieren (in der Auswahlliste auszuwählen), welche das von der VPN-Gegenstelle vorgezeigte Zertifikat signiert hat. Die weiteren CA-Zertifikate, die mit dem von der Gegenstelle vorgezeigten Zertifikat die Kette bis zum Root-CA-Zertifikat bilden, müssen aber im mGuard installiert sein - unter Menüpunkt *Authentifizierung* » *Zertifikate*.

Die Auswahlliste stellt alle CA-Zertifikate zur Wahl, die in den mGuard unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen worden sind.

Weitere Auswahlmöglichkeit:

Alle bekannten CAs

Mit dieser Einstellung werden alle VPN-Gegenstellen akzeptiert, wenn sie sich mit einem von einer CA signierten Zertifikat anmelden, das von einer bekannten CA (Certification Authority) ausgestellt ist. Bekannt dadurch, weil in den mGuard das jeweils entsprechende CA-Zertifikat und außerdem alle weiteren CA-Zertifikate geladen worden sind, so dass sie zusammen mit den vorgezeigten Zertifikaten jeweils die Kette bilden bis zum Root-Zertifikat.

B Authentifizierung durch das entsprechende Gegenstellenzertifikat:

Wählen Sie aus der Auswahlliste folgenden Eintrag:

Kein CA-Zertifikat, sondern das Gegenstellenzertifikat unten

Dann ist unten unter *Gegenstellenzertifikat* das Gegenstellenzertifikat zu installieren.

☞ Es ist nicht möglich, ein Gegenstellenzertifikat zu referenzieren, das unter Menüpunkt *Authentifizierung* » *Zertifikate* geladen ist.

Gegenstellenzertifikat

Muss konfiguriert werden, wenn die VPN-Gegenstelle per Gegenstellenzertifikat authentifiziert werden soll.

Um ein Zertifikat zu importieren, gehen Sie wie folgt vor:

Voraussetzung:

Die Zertifikatsdatei (Dateiname = *.pem, *.cer oder *.crt) ist auf dem angeschlossenen Rechner gespeichert.

Gehen Sie wie folgt vor:

1. **Durchsuchen...** klicken, um die Datei zu selektieren
2. **Hochladen** klicken.
   Danach wird der Inhalt der Zertifikatsdatei angezeigt.

VPN Identifier

Die nachfolgende Erklärung gilt, wenn die Authentifizierung der VPN-Gegenstelle anhand von CA-Zertifikaten erfolgt.

Über VPN Identifier erkennen die VPN Gateways, welche Konfigurationen zu der gleichen VPN Verbindung gehören.

Wenn der mGuard CA-Zertifikate heranzieht, um eine VPN-Gegenstellen zu authentifizieren, ist es möglich den VPN Identifier als Filter zu benutzen. Dazu ist ins nachfolgende Feld *Gegenstelle* ein entsprechender Eintrag zu machen.

Lokal

Standard: leeres Feld

Mit dem lokalen VPN-Identifier können Sie den Namen festlegen, mit dem sich der mGuard bei der Gegenstelle meldet (identifiziert). Er muss mit den Angaben aus dem Maschinenzertifikat des mGuards übereinstimmen.

Gültige Werte sind:

– Leer, also kein Eintrag (Voreinstellung). Dann wird der Subject-Eintrag (früher *Distinguished Name*) des Maschinenzertifikats verwendet.
– Der Subject-Eintrag im Maschinenzertifikat
– Einen der *Subject Alternative Name*s, wenn die im Zertifikat aufgelistet sind. Wenn das Zertifikat *Subject Alternative Name*s enthält, werden diese unter "Gültige Werte sind:" mit angegeben. Es können IP-Adressen, Hostnamen mit vorangestelltem @-Zeichen oder E-Mail-Adressen sein.

Gegenstelle

Legt fest, was im Maschinenzertifikat der VPN-Gegenstelle als Subject eingetragen sein muss, damit der mGuard diese VPN-Gegenstelle als Kommunikationspartner akzeptiert.

Durch eine entsprechende Festlegung ist es möglich, VPN-Gegenstellen, die der mGuard auf Grundlage von Zertifikatsprüfungen im Prinzip akzeptieren würde, wie folgt zu beschränken bzw. freizugeben:

- Beschränkung auf bestimmte *Subjects* (d. h. Maschinen) und/oder auf *Subjects*, die bestimmte Merkmale (Attribute) haben

oder

- Freigabe für alle *Subjects*

(Siehe dazu auch im Glossar unter „Subject, Zertifikat“.)

☞ Statt "Subject" wurde früher die Bezeichnung "Distinguished Name" verwendet.

Freigabe für alle Subjects:
Wenn Sie das Feld *Gegenstelle* leer lassen, legen Sie fest, dass im Maschinenzertifikat, das die VPN-Gegenstelle vorzeigt, beliebige Subject-Einträge erlaubt sind. Dann ist es überflüssig, das im Zertifikat jeweils angegebene Subject zu kennen oder festzulegen.

Beschränkung auf bestimmte Subjects:
Im Zertifikat wird der Zertifikatsinhaber im Feld *Subject* angegeben, das sich aus mehreren Attributen zusammensetzt. Diese Attribute werden entweder als Object Identifier ausgedrückt (z. B.: 132.3.7.32.1) oder, geläufiger, als Buchstabenkürzel mit einem entsprechenden Wert.
Beispiel: CN=VPN-Endpunkt-01, O=Beispiel GmbH, C=DE

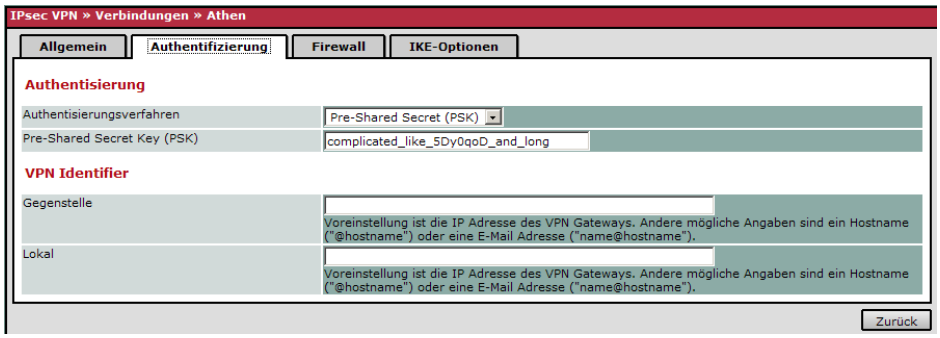
Sollen bestimmte Attribute des Subjects ganz bestimmte Werte haben, damit der mGuard die VPN-Gegenstelle akzeptiert, muss dies entsprechend spezifi-

ziert werden. Die Werte der anderen Attribute, die beliebig sein können, werden dann durch das Wildcard * (Sternchen) angegeben.
Beispiel: CN=*, O=Beispiel GmbH, C=DE
(mit oder ohne Leerzeichen zwischen Attributen)

Bei diesem Beispiel müsste im vorgezeigten Zertifikat im Subject das Attribut "O=Beispiel GmbH" und das Attribut "C=DE" stehen. Nur dann würde der mGuard den Zertifikatsinhaber (= Subject) als Kommunikationspartner akzeptieren. Die anderen Attribute könnten in den zu filternden Zertifikaten beliebige Werte haben.

☞ Wird ein Subject-Filter gesetzt, muss die Anzahl und auch die Reihenfolge der angegebenen Attribute mit der übereinstimmen, wie sie in den Zertifikaten gegeben ist, auf die der Filter angewendet werden soll.
Auf Groß- und Kleinschreibung ist zu achten.

➔ Bei Authentisierungsverfahren Pre-Shared Secret (PSK)


IPsec VPN » Verbindungen » Athen
Allgemein
Authentifizierung
Firewall
IKE-Optionen
Authentisierung
Authentisierungsverfahren
Pre-Shared Secret (PSK)
Pre-Shared Secret Key (PSK)
complicated_like_5Dy0qoD_and_long
VPN Identifier
Gegenstelle
Voreinstellung ist die IP Adresse des VPN Gateways. Andere mögliche Angaben sind ein Hostname ("@hostname") oder eine E-Mail Adresse ("name@hostname").
Lokal
Voreinstellung ist die IP Adresse des VPN Gateways. Andere mögliche Angaben sind ein Hostname ("@hostname") oder eine E-Mail Adresse ("name@hostname").
Zurück

Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei authentifizieren sich beide Seiten des VPNs über den gleichen PSK.

Um den verabredeten Schlüssel dem mGuard zur Verfügung zu stellen, gehen Sie wie folgt vor:

Ins Eingabefeld **Pre-Shared Secret Key (PSK)** die verabredete Zeichenfolge eintragen.

Um eine mit 3DES vergleichbare Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.

⌦ *Pre-Shared Secret Key* kann nicht mit dynamischen (%any) IP-Adressen verwendet werden, nur feste IP-Adressen oder Hostnamen auf beiden Seiten werden unterstützt. Hinter dem Hostnamen dürften sich aber wechselnde IP-Adressen verbergen (DynDNS).

⌦ *Pre-shared Secret Key* kann nicht verwendet werden, wenn sich mindestens einer der Kommunikationspartner (oder beide) hinter einem NAT-Gateway befinden.

VPN Identifier

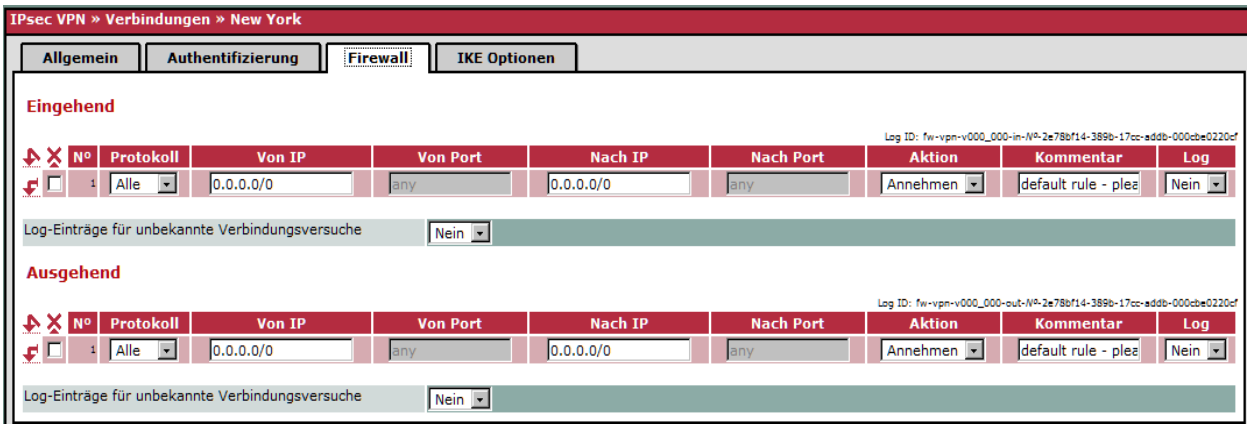
Über *VPN Identifier* erkennen die VPN Gateways, welche Konfigurationen zu der gleichen VPN Verbindung gehören.

Bei PSK sind folgende Einträge gültig:

- leer (die IP Adresse wird verwendet, dies ist die Voreinstellung)
- eine IP Adresse
- ein Hostname mit voran gestelltem ’@’ Zeichen (z. B. „@vpn1138.example.com“)

- eine E-Mail Adresse (z.B. „piepiorra@example.com“)

Firewall



Firewall eingehend (ungesicherter Port), Firewall ausgehend (gesicherter Port)

Während die unter dem Menüpunkt *Netzwerk Sicherheit* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe oben unter „Menü Netzwerksicherheit (nicht blade Kontroller)“ auf Seite 177), beziehen sich die Einstellungen hier ausschließlich auf die VPN-Verbindung, die auf diesem Registerkarten-Set definiert ist. Das bedeutet praktisch: Haben Sie mehrere VPN-Verbindungen definiert, können Sie für jede einzelne den Zugriff von außen oder von innen beschränken. Versuche, die Beschränkungen zu übergehen, können Sie ins Log protokollieren lassen.

- Gemäß werkseitiger Voreinstellung ist die VPN-Firewall so eingestellt, dass für diese VPN-Verbindung alles zugelassen ist.

  Für jede einzelne VPN-Verbindung gilt aber unabhängig voneinander gleichwohl die erweiterten Firewall-Einstellungen, die weiter oben definiert und erläutert sind - siehe „Menü Netzwerksicherheit (nicht blade Kontroller)“, „Netzwerksicherheit » Paketfilter“, „Erweiterte Einstellungen“ auf Seite 184.

- Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

- Im *Stealth*-Modus ist in den Firewallregeln die vom Client wirklich verwendete IP-Adresse zu verwenden oder aber auf 0.0.0.0/0 zu belassen, da nur ein Client durch den Tunnel angesprochen werden kann.

- Ist auf der Registerkarte ***Global*** der Schalter *Erlaube Paketweiterleitung zwischen VPN-Verbindungen* auf **Ja** gesetzt, werden für die in den mGuard eingehende Datenpakete die Regeln unter **Firewall eingehend** angewendet und für die ausgehende Datenpakete die Regeln unter **Firewall ausgehend**. Fallen die ausgehenden Datenpakete unter die selbe Verbindungsdefinition (bei einer definierten VPN-Verbindungsgruppe), werden die Firewallregeln für **Eingehend** und **Ausgehend** der selben Verbindungsdefinition angewendet. Gilt für die ausgehenden Datenpakete eine andere VPN-Verbindungsdefinition, werden die Firewallregeln für **Ausgehend** dieser anderen Verbindungsdefinition angewendet.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von IP/Nach IP

0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Eingehend:

Von IP:	die IP-Adresse im VPN-Tunnel
Nach IP	die 1-zu-1-NAT Adresse bzw. die reale Adresse

Ausgehend:

Von IP:	die 1-zu-1-NAT Adresse bzw. die reale Adresse
Nach IP:	die IP-Adresse im VPN-Tunnel

Von Port/Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

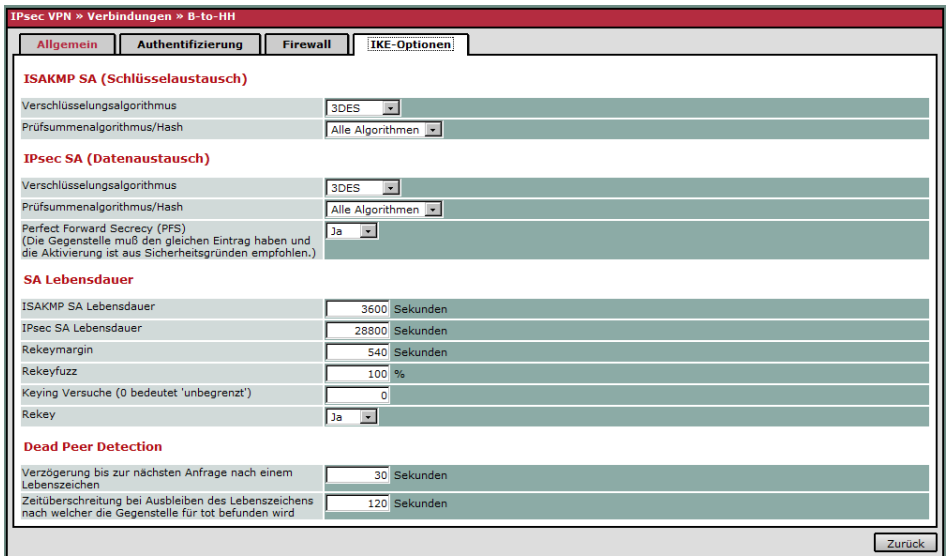
Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder nicht - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Bei **Ja** werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

IKE-Optionen



ISAKMP SA (Schlüsselaustausch)

Verschlüsselungsalgorithmus

☞ Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll.

3DES-168 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Grundsätzlich gilt Folgendes: Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das relativ neue Verfahren AES-256 gilt daher als am sichersten, ist aber noch nicht so verbreitet.

Der Verschlüsselungsvorgang ist um so zeitaufwendiger, je länger der Schlüssel ist. Dieser Gesichtspunkt spielt für den mGuard keine Rolle, weil er mit Hardware-basierter Verschlüsselungstechnik arbeitet. Jedoch könnte dieser Aspekt für die Gegenstelle eine Rolle spielen.

Der zur Auswahl stehende mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung.

Prüfsummenalgorithmus/Hash

Lassen Sie die Einstellung auf *Alle Algorithmen* stehen. Dann spielt es keine Rolle, ob die Gegenstelle mit MD5 oder SHA-1 arbeitet.

IPsec SA (Datenaustausch)

Im Unterschied zu *ISAKMP SA (Schlüsselaustausch)* (s. o.) wird hier das Verfahren für den Datenaustausch festgelegt. Es kann sich von denen des Schlüsselaustausches unterscheiden, muss aber nicht.

Verschlüsselungsalgorithmus

Siehe oben.

Prüfsummenalgorithmus/Hash

Siehe oben.

Perfect Forward Secrecy (PFS)

Verfahren zur zusätzlichen Steigerung der Sicherheit bei der Datenübertragung. Bei IPsec werden in bestimmten Intervallen die Schlüssel für den Datenaustausch erneuert. Mit PFS werden dabei mit der Gegenstelle neue

Zufallszahlen ausgehandelt, anstatt sie aus zuvor verabredeten Zufallszahlen abzuleiten.

☞ Nur wenn die Gegenstelle PFS unterstützt, wählen Sie **Ja**.

☞ Ist die Gegenstelle ein IPsec/L2TP Client, dann setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein**.

SA Lebensdauer

Die Schlüssel einer IPsec Verbindung werden in bestimmten Abständen erneuert, um die Kosten eines Angriffs auf eine IPsec Verbindung zu erhöhen.

ISAKMP SA Lebensdauer

Lebensdauer der für die ISAKMP SA vereinbarten Schlüssel in Sekunden. Werkseinstellung: 3600 Sekunden (1 Stunde). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).

IPsec SA Lebensdauer

Lebensdauer der für die IPsec SA vereinbarten Schlüssel in Sekunden.

Werkseinstellung: 28800 Sekunden (8 Stunden). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).

Rekey Margin

Minimale Zeitspanne vor Ablauf der alten Schlüssel, innerhalb der ein neuer Schlüssel erzeugt werden soll. Werkseinstellung: 540 Sekunden (9 Minuten).

Rekeyfuzz

Maximum in Prozent, um das *Rekey Margin* zufällig vergrößert werden soll. Dies dient dazu, den Schlüsselaustausch auf Maschinen mit vielen VPN-Verbindungen zeitversetzt stattfinden zu lassen. Werkseinstellung: 100 Prozent.

Keying Versuche

Anzahl der Versuche, die unternommen werden sollen, neue Schlüssel mit der Gegenstelle zu vereinbaren.

Der Wert 0 bedeutet bei Verbindungen, die der mGuard initiieren soll, unendlich viele Versuche, ansonsten 5 Versuche.

Rekey: Ja / Nein

Bei **Ja** wird der mGuard versuchen, einen neuen Schlüssel zu vereinbaren, wenn die Gültigkeit des alten abläuft.

Dead Peer Detection

Wenn die Gegenstelle das Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss.

Verzögerung bis zur nächsten Anfrage nach einem Lebenszeichen

Zeitspanne in Sekunden, nach welcher *DPD Keep Alive* Anfragen gesendet werden sollen. Diese Anfragen testen, ob die Gegenstelle noch verfügbar ist.

Werkseinstellung: 30 Sekunden.

Zeitüberschreitung bei Ausbleiben des Lebenszeichens, nach welcher die Gegenstelle für tot befunden wird

Zeitspanne in Sekunden, nach der die Verbindung zur Gegenstelle für tot erklärt werden soll, wenn auf die *Keep Alive* Anfragen keine Antwort erfolgte.

Werkseinstellung: 120 Sekunden.

☞ Wenn der mGuard eine Verbindung für tot befindet, handelt er entsprechend der Einstellung, die unter **Verbindungsinitiierung** festgelegt ist (siehe Definition dieser VPN-Verbindung, Registerkarte *Allgemein,* **Verbindungsinitiierung**).

6.9.4 IPsec VPN » L2TP über IPsec

Ermöglicht den Aufbau von VPN Verbindungen durch das IPsec/L2TP Protokoll zum mGuard.

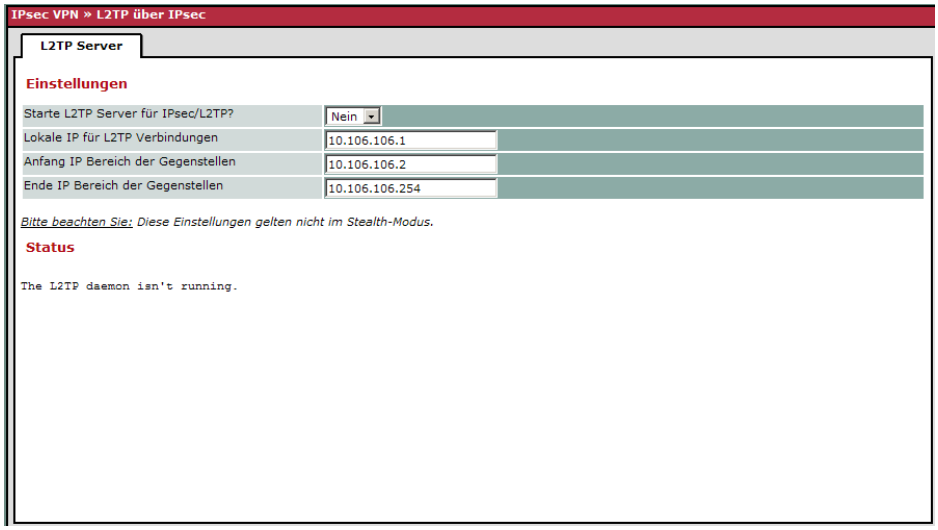
Dabei wird über eine IPsec Transportverbindung das L2TP Protokoll gefahren um darin wiederum eine Tunnelverbindung mit dem Point-to-Point-Protokoll (PPP) aufzubauen. Durch das PPP werden den Clients automatisch IP Adressen zugewiesen.

Um IPsec/L2TP zu nutzen muss der L2TP Server aktiviert werden sowie eine oder mehrere IPsec Verbindungen mit den folgenden Eigenschaften eingerichtet werden:

- **Typ**: Transport
- **Protokoll**: UDP
- **Lokaler Port**: %all
- **Remote Port**: %all
- **PFS**: Nein

(Siehe auch „→ Weitere Einstellungen nach Klicken auf Mehr...“ auf Seite 219 sowie „IKE-Optionen“ auf Seite 229.)

L2TP Server



Einstellungen

Starte L2TP Server für IPsec/L2TP? Ja / Nein

Wollen Sie IPsec/L2TP-Verbindungen ermöglichen, setzen Sie diesen Schalter auf **Ja**.

Über IPsec können dann zum mGuard L2TP Verbindungen aufgebaut werden, über welche den Clients dynamisch IP Adressen innerhalb des VPNs zugeteilt werden.

Lokale IP für L2TP Verbindungen

Nach dem obigen Screenshot teilt der mGuard der Gegenstelle mit, er habe die Adresse 10.106.106.1.

Anfang / Ende IP Bereich der Gegenstellen

Nach dem obigen Screenshot teilt der mGuard der Gegenstelle eine IP Adresse zwischen 10.106.106.2 und 10.106.106.254 mit.

Status

Informiert über den L2TP-Status, wenn dieser als Verbindungstyp gewählt ist.

6.9.5 IPsec VPN » IPsec Status

Informiert über den Status der IPsec-Verbindungen.

Links sind die Namen der VPN-Verbindungen aufgelistet, rechts daneben wird jeweils deren aktueller Status angezeigt.

Schaltflächen

Aktualisieren

Um gegebenenfalls die angezeigten Daten auf den aktuellen Stand zu bringen, auf die Schaltfläche **Aktualisieren** klicken.

Neustart

Wollen Sie eine Verbindung trennen und dann neu starten, auf die entsprechende **Neustart**-Schaltfläche klicken.

Editieren

Wollen Sie eine Verbindung neu konfigurieren, auf die entsprechende **Editieren**-Schaltfläche klicken.

Verbindung, ISAKAMP Status, IPsec Status

GATEWAY

zeigt die IP-Adressen der miteinander kommunizierenden VPN Gateways.

TRAFFIC

bezeichnet Rechner bzw. Netze, die über die VPN-Gateways kommunizieren.

ID

bezeichnet den Subject eines X.509-Zertifikats.

ISAKMP Status

ISAKMP Status (Internet security association and key management protocol) ist mit „established“ angegeben, wenn die beiden beteiligten VPN-Gateways einen Kanal zum Schlüsselaustausch aufgebaut haben. In diesem Fall konnten sie einander kontaktieren, und alle Einträge bis einschließlich „ISAKMP SA“ auf der Konfigurationsseite der Verbindung sind korrekt.

IPsec Status

IPsec Status ist mit „established“ angegeben, wenn die IPsec-Verschlüsselung bei der Kommunikation aktiviert ist. In diesem Fall sind auch die Angaben unter „IPsec SA“ und „Tunneleinstellungen“ korrekt.

Bei Problemen empfiehlt es sich, in die VPN-Logs der Gegenstelle zu schauen,

zu der die Verbindung aufgebaut wurde. Denn der initiierende Rechner bekommt aus Sicherheitsgründen keine ausführlichen Fehlermeldungen zugesandt.

Falls angezeigt wird:

ISAKMP SA established, IPsec State: WAITING

Dann bedeutet das:

Die Authentifizierung war erfolgreich, jedoch stimmten die anderen Parameter nicht: Stimmt der Verbindungstyp (Tunnel, Transport) überein? Wenn Tunnel gewählt ist, stimmen die Netzbereiche auf beiden Seiten überein?

Falls angezeigt wird:

IPsec State: IPsec SA established

Dann bedeutet das:

Die VPN-Verbindung ist erfolgreich aufgebaut und kann genutzt werden. Sollte dies dennoch nicht möglich sein, dann macht das VPN-Gateway der Gegenstelle Probleme. In diesem Fall die Verbindung deaktivieren und wieder aktivieren, um die Verbindung erneut aufzubauen.

6.10 Menü SEC-Stick

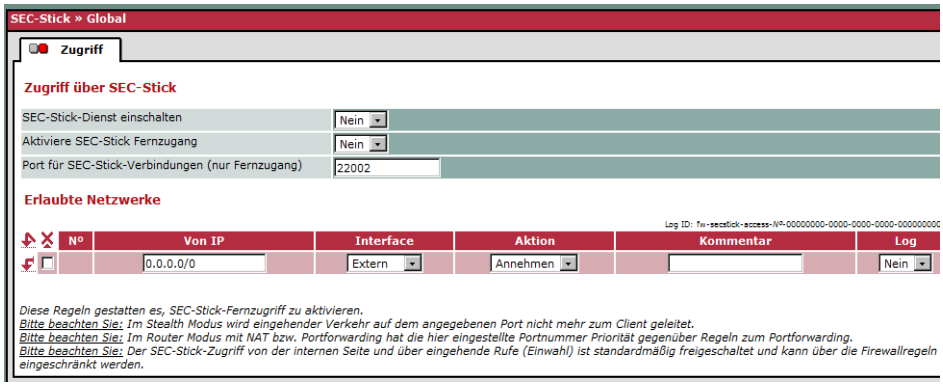
Der mGuard unterstützt die Nutzung eines SEC-Sticks, ein Zugriffsschutz für IT-Systeme. Der SEC-Stick ist ein Produkt der Firma team2work: www.team2work.de.

Der SEC-Stick ist praktisch ein Schlüssel. Der Benutzer steckt ihn in den USB-Port eines irgendwo in der Welt befindlichen Rechners mit Internetanbindung, und kann dann eine verschlüsselte Verbindung zum mGuard aufbauen, um sicher auf definierte Dienste im Netzwerk des Büros oder daheim zuzugreifen. Zum Beispiel kann das Remote Desktop Protokoll innerhalb der verschlüsselten und sicheren SEC-Stick-Verbindung benutzt werden, um den PC im Büro oder zu Hause fernzusteuern als säße er direkt davor.

Damit das funktioniert, ist der Zugang zum Geschäfts-PC durch den mGuard geschützt, und der mGuard muss für den SEC-Stick konfiguriert sein, damit dieser den Zugang öffnen kann. Denn der Benutzer des entfernten Rechners, in den der SEC-Stick eingesteckt ist, authentisiert sich beim mGuard mit den Daten und der Software, die auf seinem SEC-Stick gespeichert sind.

Der SEC-Stick stellt eine SSH-Verbindung zum mGuard her. In diese können weitere Kanäle eingebettet sein, z. B. TCP/IP-Verbindungen.

6.10.1 Global


SEC-Stick » Global
Zugriff
Zugriff über SEC-Stick
SEC-Stick-Dienst einschalten
Nein
Aktiviere SEC-Stick Fernzugang
Nein
Port für SEC-Stick-Verbindungen (nur Fernzugang)
22002
Erlaubte Netzwerke
Nº
Von IP
Interface
Aktion
Kommentar
Log
0.0.0.0/0
Extern
Annehmen
Nein
Diese Regeln gestatten es, SEC-Stick-Fernzugriff zu aktivieren.
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Der SEC-Stick-Zugriff von der internen Seite und über eingehende Rufe (Einwahl) ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Zugriff

Zugriff über SEC-Stick

⌦ Zugriff über SEC-Stick ist eine lizenzpflichtige Funktion. Sie kann nur benutzt werden, wenn die entsprechende Lizenz erworben und installiert ist.

SEC-Stick-Dienst einschalten: Ja / Nein

Mit **Ja** legen Sie fest, dass der an einem entfernten Standort eingesetzte SEC-Stick bzw. dessen Besitzer sich einloggen kann. In diesem Fall muss zusätzlich der SEC-Stick Fernzugang aktiviert werden (nächster Schalter).

Aktiviere SEC-Stick Fernzugang: Ja / Nein

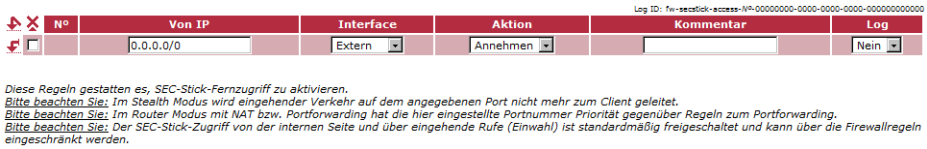
Mit **Ja** wird der SEC-Stick Fernzugang aktiviert.

Port für SEC-Stick-Verbindungen (nur Fernzugang)

Standard: 22002

Wird diese Port-Nummer geändert, gilt die geänderte Port-Nummer nur für Zugriffe über das Interface *Extern, Extern 2* oder *VPN*. Für internen Zugriff gilt weiterhin 22002.

Erlaubte Netzwerke


Log ID: fw-secstick-access-Nº-00000000-0000-0000-0000-000000000000
Nº
Von IP
Interface
Aktion
Kommentar
Log
0.0.0.0/0
Extern
Annehmen
Nein
Diese Regeln gestatten es, SEC-Stick-Fernzugriff zu aktivieren.
Bitte beachten Sie: Im Stealth Modus wird eingehender Verkehr auf dem angegebenen Port nicht mehr zum Client geleitet.
Bitte beachten Sie: Im Router Modus mit NAT bzw. Portforwarding hat die hier eingestellte Portnummer Priorität gegenüber Regeln zum Portforwarding.
Bitte beachten Sie: Der SEC-Stick-Zugriff von der internen Seite und über eingehende Rufe (Einwahl) ist standardmäßig freigeschaltet und kann über die Firewallregeln eingeschränkt werden.

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für SEC-Stick-Fernzugriff.

Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Die hier angegebenen Regeln treten nur in Kraft, wenn der Schalter **Aktiviere SEC-Stick Fernzugang** auf **Ja** steht. Weil Zugriffe von *Intern* auch möglich sind, wenn dieser Schalter auf *Nein* steht, tritt für diesen Fall eine Firewallregel, die den Zugriff von *Intern* verwehren würde, nicht in Kraft.

Sie können mehrere Regeln festlegen. Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugriff erlaubt beziehungsweise verboten ist.

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise – siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263

Interface

Extern / Intern / Extern 2 / VPN / Einwahl[1]

Gibt an, für welches Interface die Regel gelten soll.

Sind keine Regeln gesetzt oder es greift keine Regel, gelten folgende Standardeinstellungen:
SEC-Stick Fernzugang ist erlaubt über *Intern, VPN* und *Einwahl*.
Zugriffe über *Extern* und *Extern 2* werden verwehrt.

Legen Sie die Zugriffsmöglichkeiten nach Bedarf fest.

Vorsicht:

Wenn Sie Zugriffe über *Intern, VPN* oder *Einwahl* verwehren wollen, müssen Sie das explizit durch entsprechende Firewallregeln bewirken, in der Sie als Aktion z. B. *Verwerfen* festlegen.

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

1. *Extern 2* und *Einwahl* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

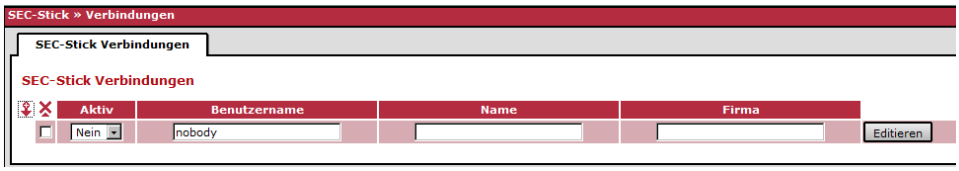
Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

6.10.2 Verbindungen



SEC-Stick Verbindungen

SEC-Stick Verbindungen

Liste der definierten SEC-Stick-Verbindungen. Wollen Sie eine neue Verbindnug hinzufügen klicken sie links oben auf den Pfeil nach unten. Eine bereits bestehende Verbindung können Sie bearbeiten, indem Sie auf die Schaltfläche **Editieren** klicken.

Aktiv: Ja / Nein

Um eine definierte SEC-Stick Verbindung nutzen zu können, muss der Schalter **Aktiv** auf **Ja** gesetzt werden.

Benutzername

Für jeden zugriffsberechtigten Inhaber eines SEC-Sticks, muss eine SEC-Stick Verbindung mit einem eindeutig zugeordneten Benutzernamen definiert werden. Anhand dieses Benutzernamens werden die definierten Verbindungen eindeutig identifiziert.

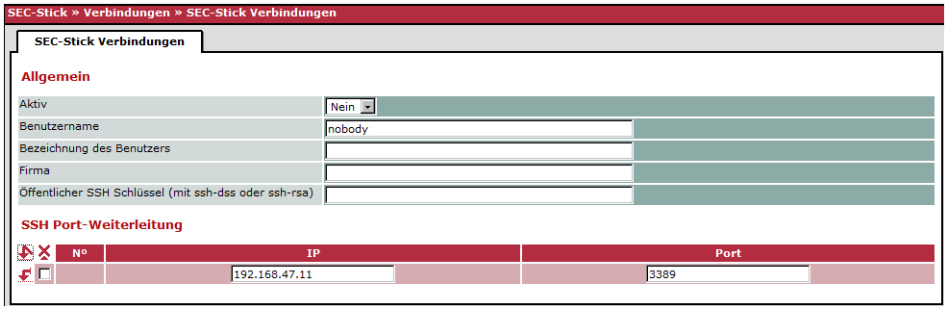
Name

Name der Person.

Firma

Angabe der Firma.

Nach Klicken auf Editieren erscheint folgende Seite:



Allgemein

Aktiv: Ja / Nein

Wie oben

Benutzername

Wie oben

Bezeichnung des Benutzers

Name der Person. (Wiederholt)

Firma

Wie oben

Öffentlicher SSH-Schlüssel (mit ssh-dss oder ssh-rsa)

Hier muss der öffentliche SSH-Schlüssel, der zum SEC-Stick gehört, im ASCII-Format eingetragen werden. Das geheime Gegenstück ist auf dem SEC-Stick gespeichert.

SSH Port-Weiterleitung

Liste der erlaubten Zugriffe und SSH-Port Weiterleitungen bezogen auf den SEC-Stick des entsprechenden Benutzers.

IP

Die IP-Adresse des Rechners, auf den der Zugriff ermöglicht wird.

Port

Port-Nummer, die beim Zugriff auf den Rechner benutzt werden soll.

⌦ Nicht alle Funktionen des SEC-Stick können über die Web-Benutzeroberfläche des mGuard konfiguriert werden.

6.11 Menü QoS

QoS (Quality of Service) bezeichnet die Dienstgüte einzelner Übertragungskanäle in IP-Netzwerken. Dabei geht es um die Zuteilung bestimmter Ressourcen an bestimmte Dienste (Services) bzw. Kommunikationsarten, damit diese reibungslos funktionieren. So muss z. B. für die Übertragung von Audio- oder Videodaten in Realzeit die notwendige Bandbreite bereitgestellt werden, um eine zufriedenstellende Kommunikation zu erreichen, während ein eventuell langsamerer Datentransfer per FTP oder E-Mail unkritisch für den gewünschten Gesamterfolg (Übertragung der gewünschten Datei oder E-Mail) ist.

6.11.1 Ingress Filter

Ein Ingress Filter bewirkt, dass bestimmte Datenpakete vor Eintreten in den Verarbeitungsmechanismus des mGuard ausgefiltert und verworfen werden, so dass eine Verarbeitung nicht stattfindet. Der mGuard kann Ingress-Filter benutzen, um die vorhandene Verarbeitungsleistung nach Möglichkeit nicht mit solchen Datenpaketen zu belasten, die im Netzwerk nicht gebraucht werden. Das hat den Effekt, dass die anderen, d. h. die gebrauchten Datenpakete schneller verarbeitet werden.

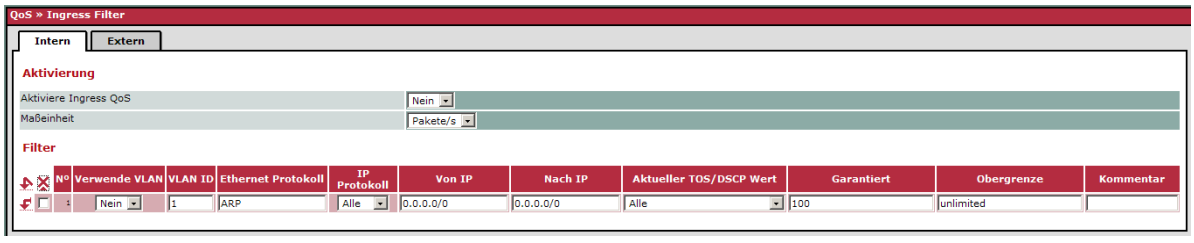
Durch geeignete Filterregeln kann z. B. sichergestellt werden, dass der administrative Zugang zum mGuard immer mit hoher Wahrscheinlichkeit erfolgen kann.

Die Paketverarbeitung auf dem mGuard ist im Wesentlichen durch das Handling des einzelnen Datenpakets geprägt, so dass die Verarbeitungsleistung nicht von der Bandbreite sondern von der Zahl der zu verarbeitenden Pakete abhängt.

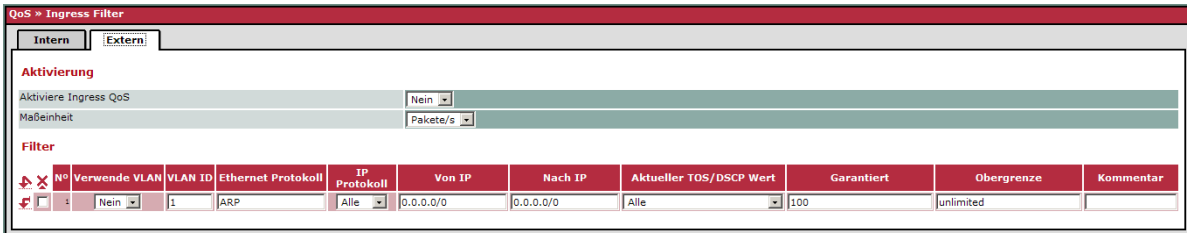
Gefiltert wird ausschließlich nach Merkmalen, die jedes einzelne Datenpaket aufweist oder aufweisen kann: die im Header angegebene IP-Adresse von Sender und Absender, das angegebene Ethernet-Protokoll, das angegebene IP-Protokoll, der angegebene TOS/DSCP Wert und/oder die VLAN ID, wenn VLANs eingerichtet sind. Da durch die gesetzten Filterregeln bei jedem einzelnen Datenpaket geprüft wird, ob es unter die Filterregeln fällt, sollte die Liste der Filterregeln kurz sein. Sonst könnte die Zeit, die zum Ausfiltern gebraucht wird, länger sein, als der durch das Ausfiltern erzielte Zeitgewinn.

Es ist zu beachten, dass nicht alle angebbaren Filterkriterien sinnvoll kombiniert werden können. Zum Beispiel macht es keinen Sinn, bei Angabe des Ethernet-Protokolls ARP im selben Regelsatz zusätzlich ein IP Protokoll anzugeben. Oder bei Angabe des Ethernet Protokolls IPX (hexadezimal anzugeben) die IP Adressen von Sender oder Absender vorzugeben.

Intern / Extern



Intern: Einstellung für Ingress Filter an der LAN-Schnittstelle



Extern: Einstellung für Ingress Filter an der WAN-Schnittstelle

Aktivierung

Aktiviere Ingress QoS: Ja / Nein

Nein (Standard): Das Feature ist ausgeschaltet. Falls Filterregeln definiert sind, werden sie ignoriert.

Ja: Das Feature ist eingeschaltet. Datenpakete dürfen nur dann passieren und werden der Weitervermittlung und -verarbeitung des mGuard zugeführt, wenn sie den nachfolgend festgelegten Filterregeln entsprechen.

Filter können für den LAN-Port (Registerkarte **Intern**) und den WAN-Port (Registerkarte **Extern**) gesetzt werden.

Maßeinheit: kbit/s / Pakete/s

Legt fest, in welcher Maßeinheit die weiter unten unter **Garantiert** und **Obergrenze** anzugebenden Zahlenwerte zu verstehen sind.

Filter

Verwende VLAN: Ja / Nein

Ist ein VLAN eingerichtet, kann die betreffende VLAN ID angegeben werden, damit die betreffenden Datenpakete passieren dürfen. Dazu muss dieser Schalter auf **Ja** stehen.

VLAN ID

Legt fest, dass die Datenpakete des VLANs, das diese VLAN ID hat, passieren dürfen. (Dazu muss der Schalter **Verwende VLAN** auf **Ja** stehen.)

Ethernet Protokoll

Legt fest, dass nur Datenpakete des angegebenen Ethernet Protokolls passieren dürfen. Mögliche Einträge: **ARP**, **IPV4**, **%any**. Anderer Angaben müssen hexadezimal (bis zu 4 Ziffern) eingetragen werden.

(Bei den Angaben handelt es sich um die Kennung des betreffenden Protokolls, die im Ethernet-Header steht. Kann in den Veröffentlichungen des betreffenden Standards nachgeschlagen werden.)

IP Protokoll: Alle / TCP / UDP / ICMP / ESP

Legt fest, dass nur Datenpakete des ausgewählten IP Protokolls passieren dürfen. Mit **Alle** findet keine Filterung nach IP Protokoll statt.

Von IP

Legt fest, dass nur Datenpakete passieren dürfen, die von der angegebenen IP-Adresse kommen.

Die Angabe **0.0.0.0/0** steht für alle Adressen, d. h. in diesem Fall findet keine Filterung nach IP-Adresse des Absenders statt. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263

Nach IP

Legt fest, dass nur solche Datenpakete passieren dürfen, die zur angegebenen IP-Adresse weitergeleitet werden sollen.

Angabe entsprechend wie oben unter *Von IP*.

Die Angabe **0.0.0.0/0** steht für alle Adressen, d. h. in diesem Fall findet keine Filterung nach IP-Adresse des Absenders statt.

Aktueller TOS/DSCP Wert

Jedes Datenpaket enthält ein TOS bzw. DSCP Feld. (TOS steht für Type Of Service, DSCP für Differentiated Services Code Point.) Hier wird angegeben, zu welcher Art von Traffic das Datenpaket gehört. So wird z. B. ein IP-Telefon in dieses Feld der von ihm ausgehenden Datenpakete etwas anderes hineinschreiben als ein FTP-Programm.

Wenn Sie hier einen Wert auswählen, dürfen nur die Datenpakete passieren, die in ihrem TOS-bzw. DSCP-Feld diesen Wert haben. Mit **Alle** findet keine Filterung nach TOS/DSCP Wert statt.

Garantiert

Die anzugebende Zahl legt fest, wie viele Datenpakete/s bzw. kbit/s - je nach eingestellter **Maßeinheit** (s. o.) - auf jeden Fall passieren dürfen. Das gilt für den Datenstrom, der den links angegebenen Kriterien dieses Regelsatzes entspricht, also passieren darf. Liefert dieser Datenstrom mehr Datenpakete pro Sekunde, dann darf der mGuard bei Kapazitätsengpässen die überzählige Anzahl an Datenpaketen verwerfen.

Obergrenze

Die anzugebende Zahl legt fest, wie viele Datenpakete/s bzw. kbit/s - je nach eingestellter **Maßeinheit** (s. o.) - maximal passieren dürfen. Das gilt für den Datenstrom, der den links angegebenen Kriterien dieses Regelsatzes entspricht, also passieren darf. Liefert dieser Datenstrom mehr Datenpakete pro Sekunde, dann verwirft der mGuard die überzählige Anzahl an Datenpaketen.

Kommentar

Optional: kommentierender Text.

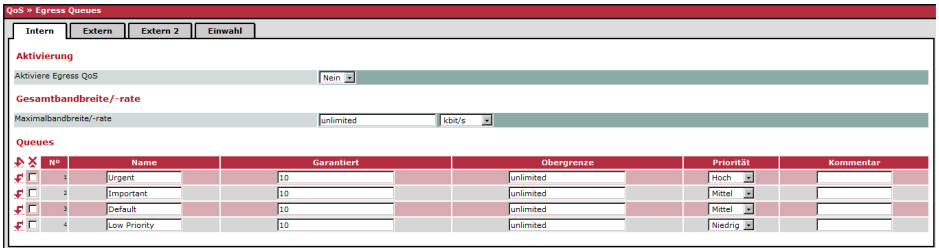
6.11.2 Egress Queues

Den Diensten werden entsprechende Prioritätsstufen zugeordnet. Bei Verbindungsengpässen werden dann je nach zugeordneter Prioritätsstufe die ausgehenden Datenpakete in Egress Queues (= Warteschlangen für anstehende Pakete) gestellt, die mit entsprechender Priorität abgearbeitet werden. Die Zuordnung von Prioritätsstufe und Bandbreite sollte im Idealfall so erfolgen, dass für Datenpakete von in Realzeit zu vollziehenden Übertragungen immer genügend Bandbreite zur Verfügung steht, während Pakete von anderen wie z. B. FTP-Downloads im Ernstfall vorübergehend auf Warten gesetzt werden.

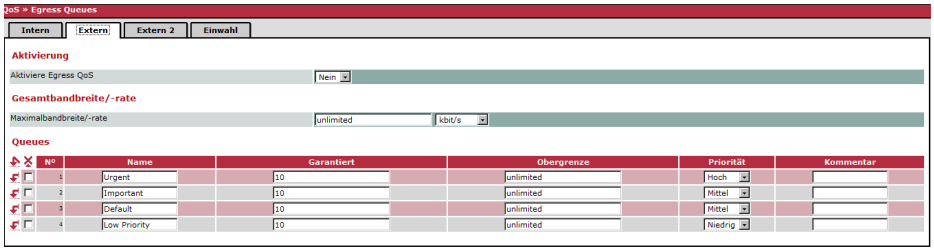
Die Hauptanwendung von Egress QoS ist die optimale Ausnutzung der zur Verfügung stehenden Bandbreite am jeweiligen Anschluss. In einigen Fällen kann auch eine Begrenzung der Paketrate nützlich sein, z. B. um einen langsamen Rechner im geschützten Netz vor Überlast zu schützen.

Das Feature *Egress Queues* kann für alle Schnittstellen eingesetzt werden und für VPN-Verbindungen.

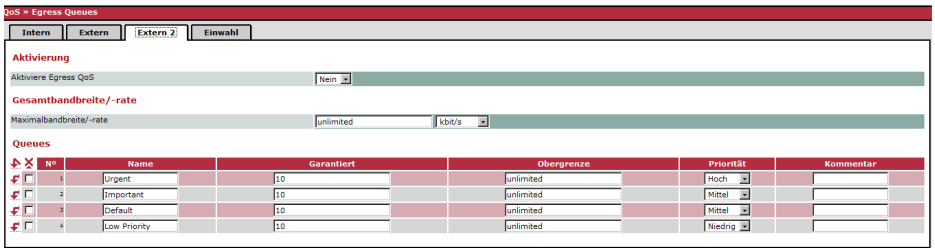
Intern / Extern / Extern 2 / Einwahl



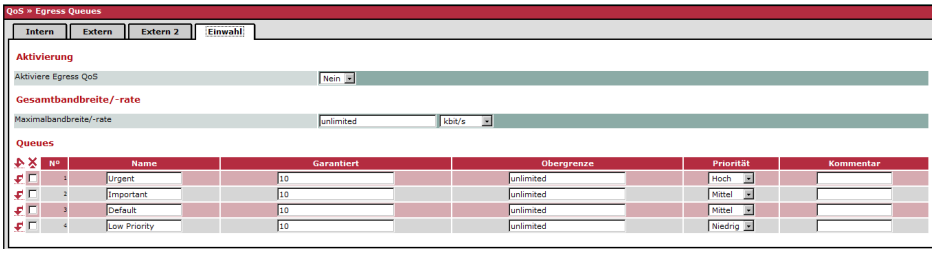
Intern: Einstellung für Egress Queues an der LAN-Schnittstelle



Extern: Einstellung für Egress Queues an der WAN-Schnittstelle Extern



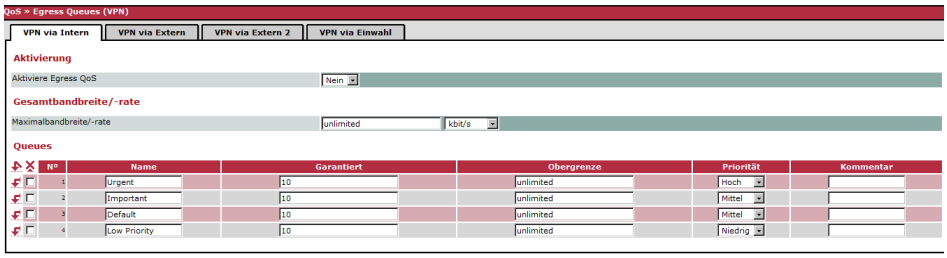
Extern 2: Einstellung für Egress Queues bei der sekundären externen Schnittstelle.



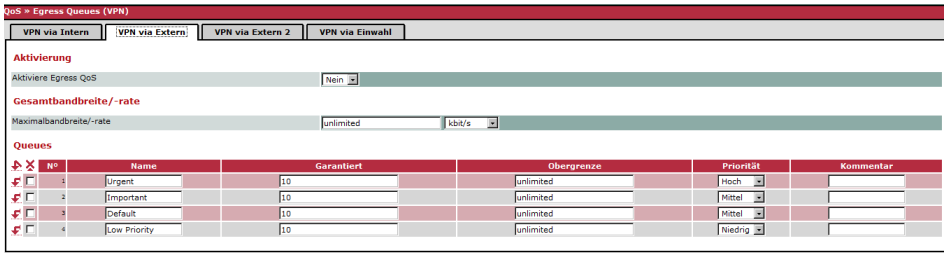
Einwahl: Einstellung für Egress Queues für Pakete für ppp-Wählverbindung (Einwahl)

6.11.3 Egress Queues (VPN)

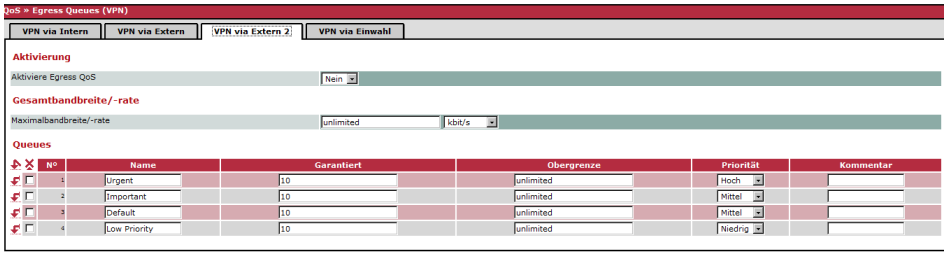
VPN via Intern /
VPN via Extern /
VPN via Extern 2 /
VPN via Einwahl



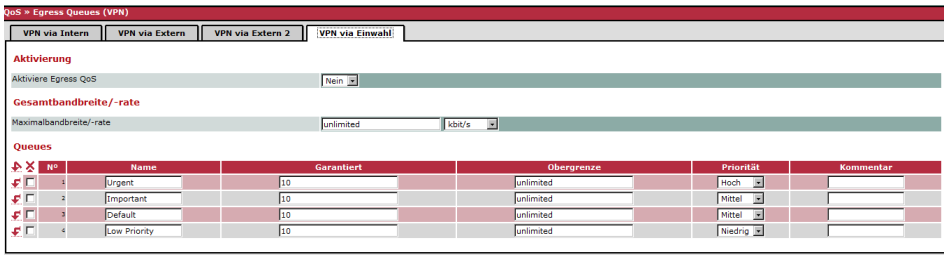
VPN via Intern: Einstellung für Egress Queues



VPN via Extern: Einstellung für Egress Queues



VPN via Extern 2: Einstellung für Egress Queues



VPN via Einwahl: Einstellung für Egress Queues

Alle oben aufgeführten Registerkarten für *Egress Queues* bei den Interfaces *Intern, Extern, Extern 2, Einwahl* sowie für VPN-Verbindungen, die über dieses Interfaces geführt werden, bieten die gleichen Einstellmöglichkeiten.

In allen Fällen beziehen sich die Einstellungen auf die Daten, die von der jeweiligen Schnittstelle gesehen vom mGuard nach außen ins Netz gehen.

Aktivierung

Aktiviere Egress QoS: Ja / Nein

Nein (Standard): Das Feature ist ausgeschaltet.

Ja: Das Feature ist eingeschaltet. Empfiehlt sich dann, wenn die Schnittstelle an ein Netz mit geringer Bandbreite angeschlossen ist, so dass eine Beeinflussung der Bandbreitenzuordnung zugunsten besonders wichtiger Daten gewünscht wird.

Gesamtbandbreite

Maximalbandbreite/-rate ..... kBit/s / Pakete/s

Bandbreite, die insgesamt maximal physikalisch zur Verfügung steht - anzugeben in kBit/s oder Pakete/s.

Die hier angegebene Gesamtbandbreite sollte etwas geringer angegeben werden als tatsächlich vorhanden, damit die Priorisierung optimal arbeitet. Damit wird verhindert, dass Puffer von weitervermittelnden Geräten überlaufen können und dadurch einen unerwünschten Effekt erzeugen.

Queues

Name

Sie können die voreingestellten Namen für die Egress Queues übernehmen oder andere vergeben. Die Namen legen nicht die Prioritätsstufe fest.

Garantiert

Bandbreite, die der betreffenden Queue auf jeden Fall zur Verfügung stehen soll. Je nach dem, ob oben unter **Maximalbandbreite/-rate** diese in **kbit/s** ODER in **Pakete/s** angegeben ist, verwenden Sie auch hier die selbe Maßeinheit, ohne diese explizit anzugeben.
Die Summe aller garantierten Bandbreiten muss in Bezug zur Gesamtbandbreite kleiner oder gleich sein.

Obergrenze

Bandbreite, die der betreffenden Queue vom System maximal zur Verfügung gestellt werden darf. Je nach dem, ob oben unter **Maximalbandbreite/-rate** diese in **kbit/s** ODER in **Pakete/s** angegeben ist, verwenden Sie auch hier die selbe Maßeinheit, ohne diese explizit anzugeben.
Der Wert muss größer sein als die garantierte Bandbreite oder dieser gleich sein. Es kann auch der Wert **unlimited** angegeben werden, der keine weitere Beschränkung bewirkt.

Priorität: Niedrig / Mittel / Hoch

Legt fest, mit welcher Priorität die betreffende Warteschlange, sofern vorhanden, abgearbeitet werden muss, falls die zur Verfügung stehende Gesamtbandbreite aktuell nicht ausgeschöpft ist.

Kommentar

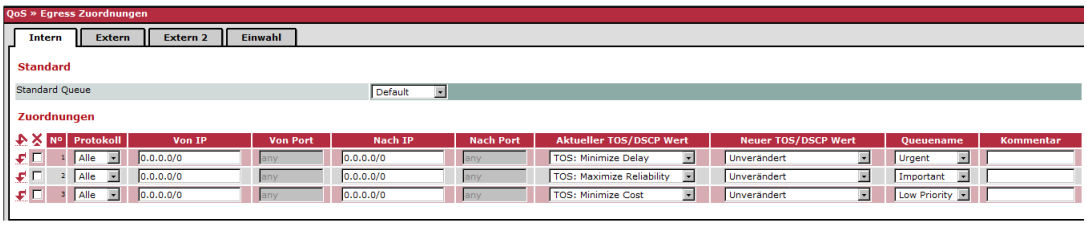
Optional: kommentierender Text.

6.11.4 Egress Zuordnungen

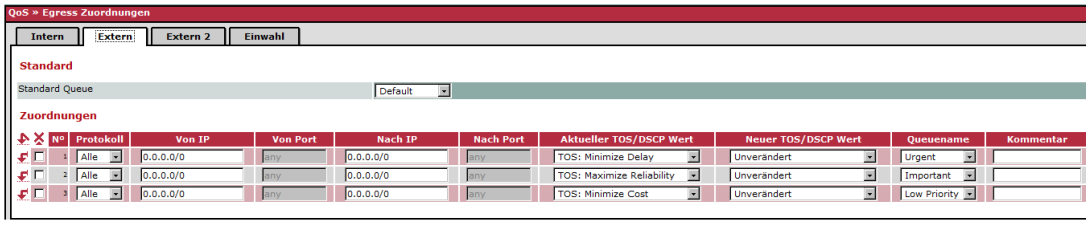
Welche Daten werden den definierten Egress Queues (= Warteschlangen) (s. o.) zugeordnet, damit sie mit der Priorität übertragen werden, die der jeweiligen Queue zugeteilt ist?

Die Zuordnungen können bezüglich aller Schnittstellen sowie für VPN-Verbindungen separat festgelegt werden.

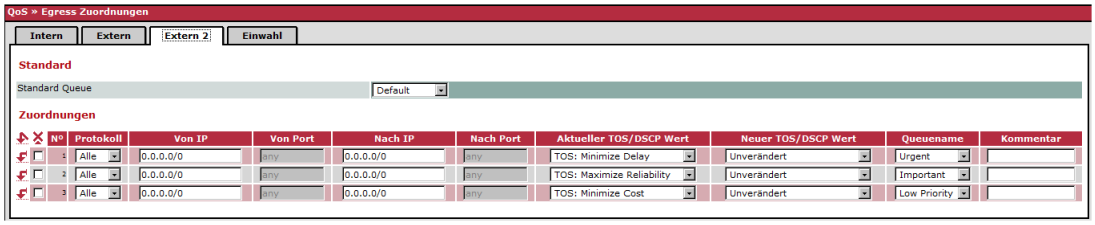
Intern / Extern / Extern2 / Einwahl



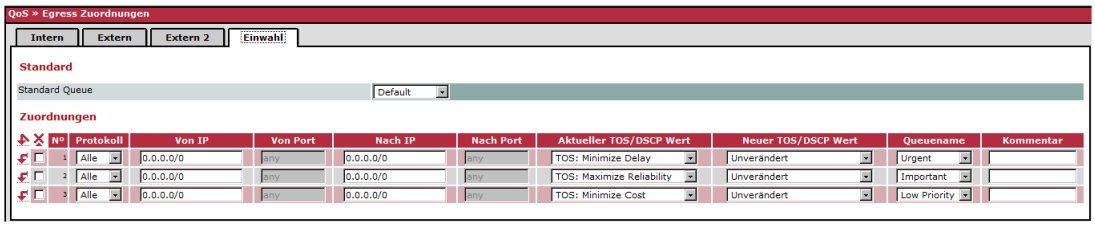
Intern: Einstellung für Egress Queue Zuordnungen



Extern: Einstellung für Egress Queue Zuordnungen



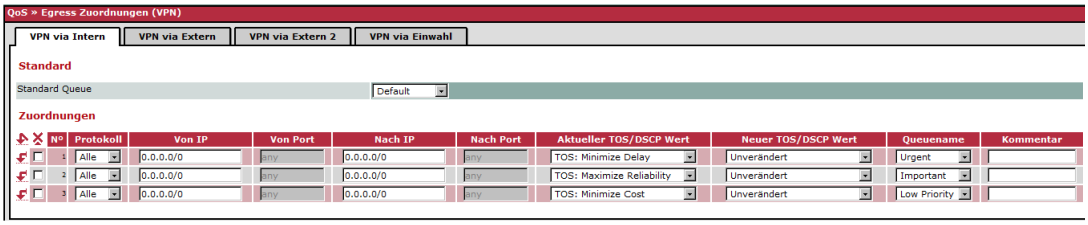
Extern 2: Einstellung für Egress Queue Zuordnungen



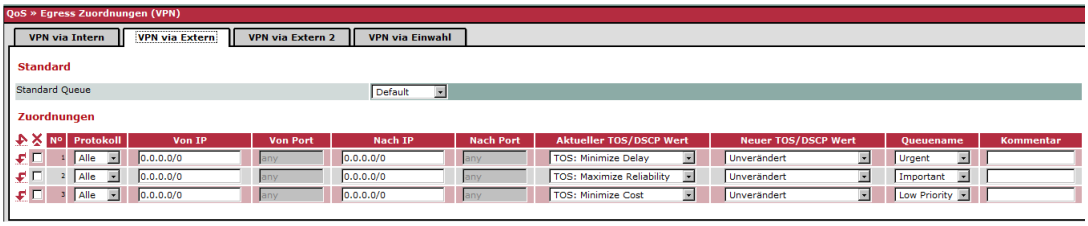
Einwahl: Einstellung für Egress Queue Zuordnungen

6.11.5 Egress Zuordnungen VPN

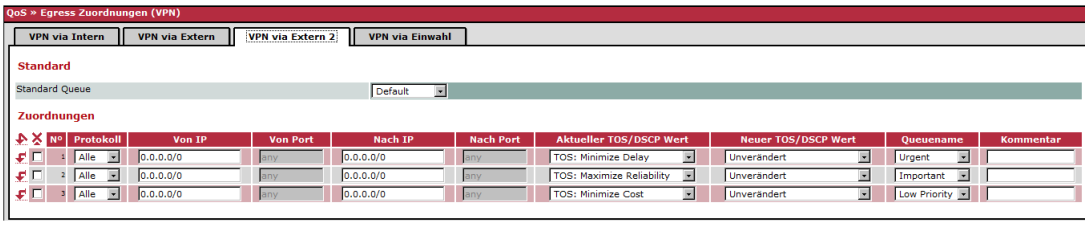
VPN via Intern /
VPN via Extern /
VPN via Extern2 /
VPN via Einwahl



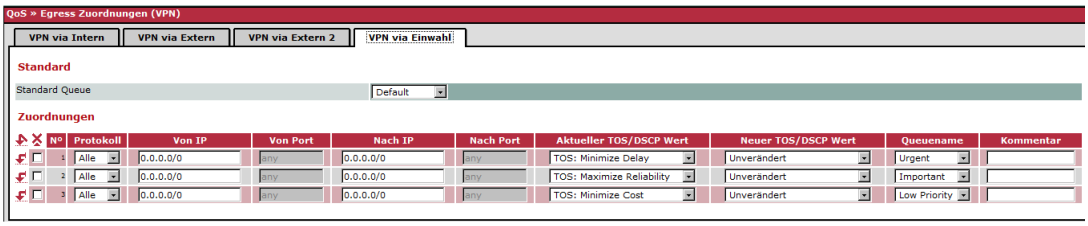
VPN via Intern: Einstellung für Egress Queue Zuordnungen



VPN via Extern: Einstellung für Egress Queue Zuordnungen



VPN via Extern 2: Einstellung für Egress Queue Zuordnungen



VPN via Einwahl: Einstellung für Egress Queue Zuordnungen

Alle oben aufgeführten Registerkarten für *Egress Zuordnungen* in Bezug auf die Interfaces *Intern, Extern, Extern 2, Einwahl* sowie für VPN-Verbindungen, die über diese Interfaces geführt werden, bieten die gleichen Einstellmöglichkeiten.

In allen Fällen beziehen sich die Einstellungen auf die Daten, die von der jeweiligen Schnittstelle gesehen vom mGuard nach außen ins Netz gehen.

Standard

Standard Queue: *Namen der Egress Queues* **(benutzerdefiniert)**

Angezeigt werden die Namen der Queues, wie sie unter *Egress Queues* auf den Registerkarten *Intern* / *Extern* / *VPN via Extern* angezeigt oder festgelegt sind. Standardmäßig sind das folgende Namen: Default / Urgent / Important / Low Priority

Traffic, der nicht nachfolgend unter *Zuordnungen* einer bestimmten Egress Queue zugeordnet wird, bleibt der *Standard Queue* zugeordnet. Über diese Auswahlliste legen Sie fest, welche Egress Queue als *Standard Queue* gelten soll.

Zuordnungen

Die Zuordnung bestimmten Daten-Traffics zu einer Egress Queue erfolgt über eine Liste von Kriterien. Treffen die Kriterien einer Zeile auf ein Datenpaket zu, wird es in die dort benannte Egress Queue eingeordnet.

Beispiel:

Sie haben für zu übertragende Audio-Daten unter QoS » Egress Queues (siehe „Egress Queues“ auf Seite 243) unter dem Namen *Urgent* eine Queue mit garantierter Bandbreite und Priorität definiert. Dann legen Sie hier fest, nach welchen Regeln Audio-Daten erkannt werden, und dass diese Daten zur Queue *Urgent* gehören sollen.

Protokoll: Alle / TCP / UDP / ICMP /ESP

Protokoll(e), auf das/die sich die Zuordnung bezieht.

Von IP

IP-Adresse des Netzes/Geräts, von wo die Daten kommen.
0.0.0.0/0 bedeutet alle IP-Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 263.

Den Traffic von dieser Quelle ordnen Sie weiter hinten in dieser Zeile der Queue zu, die Sie unter *Queuename* auswählen.

Von Port

Benutzter Port bei der Quelle, von wo die Daten kommen (wird nur ausgewertet bei den Protokollen TCP und UDP).

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Nach IP

IP-Adresse des Netzes/Geräts, wohin die Daten gehen. Angabe entsprechend wie oben unter *Von IP*.

Nach Port

Benutzter Port bei der Quelle, wohin die Daten gehen. Angabe entsprechend wie oben unter *Von Port.*

Aktueller TOS/DSCP Wert

Jedes Datenpaket enthält ein TOS bzw. DSCP Feld. (TOS steht für Type Of Service, DSCP für Differentiated Services Code Point.) Hier wird angegeben, zu welcher Art von Traffic das Datenpaket gehört. So wird z. B. ein IP-Telefon in dieses Feld der von ihm ausgehenden Datenpakete etwas anderes hineinschreiben als ein FTP-Programm, das Datenpakete auf einen Server hochlädt.

Wenn Sie hier einen Wert auswählen, werden nur die Datenpakete genommen, die in ihrem TOS-bzw. DSCP-Feld diesen Wert haben, um sie - je nach Eintrag im Feld **Neuer TOS/DSCP-Wert** - auf einen anderen Wert zu setzen.

Neuer TOS/DSCP-Wert

Wenn Sie den TOS/DSCP-Wert der Datenpakete ändern wollen, die anhand der gegebenen Regeln selektiert sind, wählen Sie hier aus, was ins TOS- bzw. DSCP-Feld geschrieben werden soll.

Weitere Erläuterungen zu **Aktueller TOS/DSCP Wert** und **Neuer TOS/DSCP-Wert** finden Sie in folgenden RFC-Dokumenten

- RFC3260 "New Terminology and Clarifications for Diffserv"
- RFC3168 "The Addition of Explicit Congestion Notification (ECN) to IP"
- RFC2474 "Definition of the Differentiated Services Field (DS Field)"
- RFC1349 "Type of Service in the Internet Protocol Suite"

Queuename

Name der Egress Queue, welcher der Traffic zugeordnet werden soll.

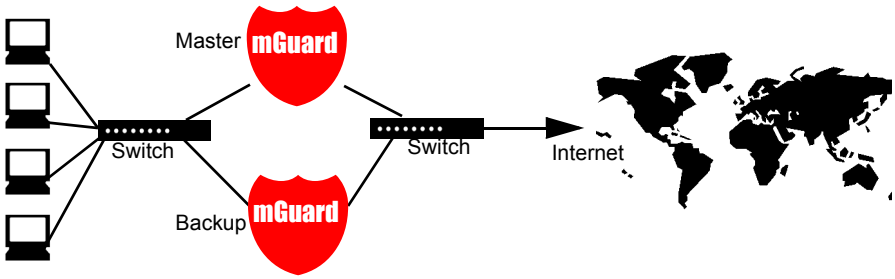
Kommentar

Optional: kommentierender Text.

6.12 Menü Redundanz

6.12.1 Firewall-Redundanz

Mit Hilfe der Redundanzfähigkeit ist es möglich, zwei mGuards zu einem einzigen virtuellen Router zusammenzufassen.



Dabei übernimmt der zweite mGuard (Backup) in einem Fehlerfall die Funktion des ersten mGuard (Master).

Dazu wird der Zustand der Stateful Firewall zwischen beiden mGuards fortwährend synchronisiert, so dass bei einem Wechsel bestehende Verbindungen nicht abgebrochen werden.

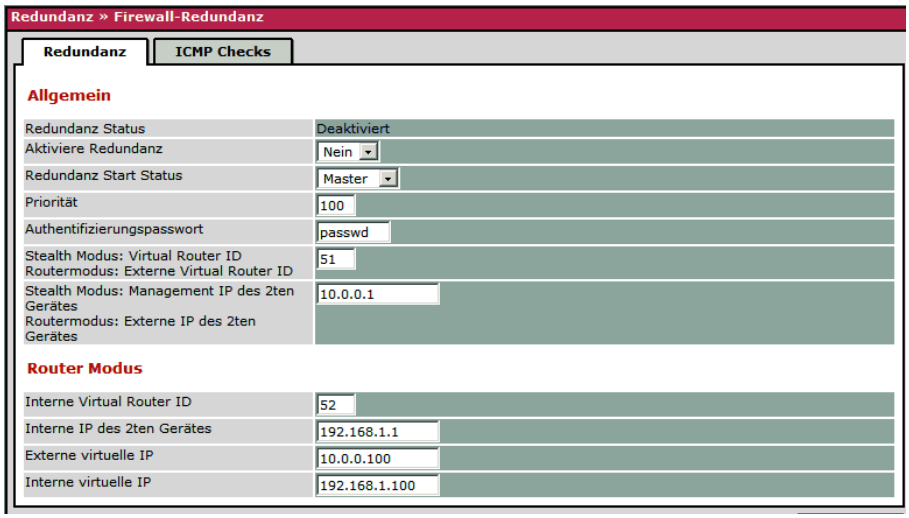
- Voraussetzung: Beide mGuards müssen entsprechend konfiguriert werden. Die Firewalleinstellungen sollten identisch sein, damit nach der Umschaltung keine Probleme auftreten.
- Redundanz wird in folgenden Netzwerkmodi unterstützt: *Router-Modus, Stealth-Modus statisch* mit Management IP und im *Stealth-Modus (mehrere Clients)*.
- Redundanz wird nicht bei aktiviertem Interface *Extern 2*[1] unterstützt.
- Werden die beiden mGuards im Netzwerkmodus *Stealth-Modus statisch* mit Management IP oder im *Stealth-Modus (mehrere Clients) betrieben,* werden DAD ARP Anfragen auf dem internen Interface versendet, wenn der eine mGuard die Funktion des anderen übernimmt, siehe RFC2131, Abschnitt 4.4.1.
- Bei aktivierter Redundanz dürfen die beiden mGuards nicht als VPN-Gateway genutzt werden.
- Bei aktivierter Redundanz können die Benutzerfirewall-Logins nicht zwischen den mGuards synchronisiert werden. Auf der virtuellen IP-Adresse stellt der mGuard keine Benutzeroberfläche zur Verfügung. Darum ist es nicht möglich, sich dort als Benutzer der Benutzerfirewall anzumelden.
- Bei Geräten, die am LAN-Port des mGuards angeschlossen sind, muss die interne virtuelle IP-Adresse (s.u.) der mGuards als Standardgateway konfiguriert werden.

Die folgenden Funktionen können bei aktivierter Redundanz genutzt werden - siehe „Menü Netzwerksicherheit (nicht blade Kontroller)“:

- Eingehende/ausgehende Firewall Regeln
- NAT (IP-Masquerading, d. h. ausgehender Netzwerkverkehr wird auf die externe virtuelle IP umgeschrieben.)

1. *Extern 2* nur bei Geräten mit serieller Schnittstelle. Siehe „Netzwerk » Interfaces“ auf Seite 109.

- 1:1 NAT
- Port Weiterleitung (für *Eingehend auf IP* muss die externe virtuelle IP konfiguriert werden)
- MAC-Filter



Redundanz

Allgemein

Redundanz Status

Zeigt den aktuellen Status an.

Aktiviere Redundanz: Ja/ Nein

Redundanz aktivieren/deaktivieren.

Redundanz Start Status

Status des mGuards bei Aktivierung der Redundanz (*Master* oder *Backup*).

Priorität

Entscheidet, welcher mGuard als Master fungiert.

Sind die Prioriäten unterschiedlich gesetzt, so arbeitet der mGuard mit der höheren Priorität als Master, solange er nicht ausfällt.

Haben beide mGuards die gleiche Priorität und wird im Fehlerfall der Backup zum Master, so arbeitet dieser auch dann als Master weiter, wenn der vorherige mGuard wieder zur Verfügung steht.

Werte zwischen 1 und 254 sind möglich.

Authentifizierungspasswort

Das Passwort soll vor Fehlkonfigurationen schützen, bei denen sich mehrere virtuelle Router gegenseitig stören.

Das Passwort muss auf beiden mGuards gleich sein. Es wird im Klartext übermittelt und sollte daher nicht identisch mit anderen sicherheitsrelevanten Passwörtern sein.

Stealth-Modus: Virtual Router ID
Router-Modus: Externe Virtual Router ID

Eine ID zwischen 1 und 255, die auf beiden mGuards gleich sein muss und den virtuellen Router identifiziert.

Stealth-Modus: Management IP des 2ten Gerätes

Router-Modus: Externe IP des 2ten Gerätes

Im Stealth-Modus die Management IP des zweiten mGuards, im Router-Modus die IP-Adresse des WAN-Ports des zweiten mGuards.

Router Modus

Die folgenden Werte müssen gesetzt werden, wenn die mGuards im Router Modus betrieben werden.

Interne Virtual Router ID

Eine ID zwischen 1 und 255, die auf beiden mGuards gleich sein muss. Diese ID identifiziert den virtuellen Router am LAN-Port.

Interne IP des 2ten Gerätes

IP-Adresse des LAN-Ports des zweiten mGuards.

Externe virtuelle IP

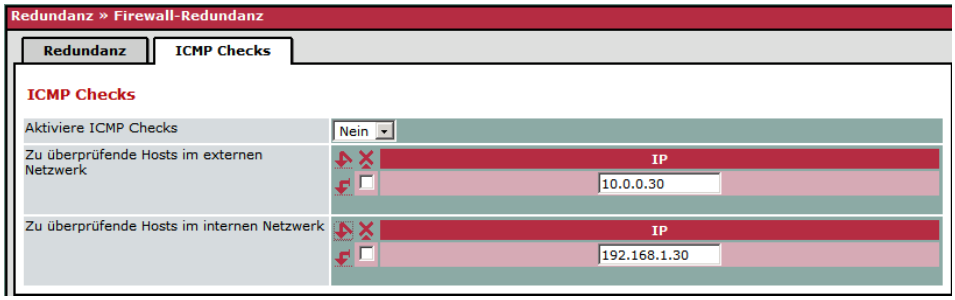
Virtuelle IP-Adresse, über die der Verkehr durch den mGuard läuft. Wird z. B. bei NAT als externe IP verwendet. Kann beliebig festgelegt werden, sofern sie tatsächlich im extern konfigurierten Netz ist und sich nicht mit einer anderen IP-Adresse dort überschneidet.

Interne virtuelle IP

Virtuelle IP-Adresse, über die der Verkehr durch den mGuard läuft. Diese muss z. B. bei den Clients, die sich im am LAN-Port des mGuard angeschlossenen Netzwerk befinden, als Standardgateway eingestellt werden.

Kann beliebig festgelegt werden, sofern sie tatsächlich im intern konfigurierten Netz ist und sich nicht mit einer anderen IP-Adresse dort überschneidet.

ICMP Checks



ICMP Checks bilden eine zusätzliche Möglichkeit der Überwachung der Netzwerkverbindungen zwischen den mGuards, die als virtueller Router zusammenarbeiten.

Fällt eine der beiden direkten Ethernet-Verbindungen aus, die zwischen den LAN-Ports der beiden mGuards besteht (in der Zeichnung auf Seite 250 links von den beiden mGuards) und zwischen ihren WAN-Ports (in der Zeichnung rechts von den beiden mGuards), dann wird der Backup zum Master. Das vom mGuard verwendete Virtual Router Redundancy Protocol (VRRP) kann den noch funktionierenden Master jedoch nicht darüber informieren. Über die noch funktionierenden Netzwerkverbindung würden die zwei Master anschließend miteinander in Konflikt stehen.

Über die ICMP Checks (ICMP Ping) kann der Master daher die Verbindung zum Backup überprüfen und sich gegebenenfalls deaktivieren.

Aktiviere ICMP Checks: Ja / Nein

Bei **Ja** wird die Verbindung zum Backup mit Hilfe des ICMP Protokolls überwacht.

Ist der Backup mGuard nicht mehr zu erreichen, versucht der Master nacheinander die Hosts zu erreichen, die unter *Zu überprüfende Hosts im externen/ internen Netzwerk* angegebenen sind.

Sind auch diese nicht erreichbar, deaktiviert sich der Master.

Zu überprüfende Hosts im externen Netzwerk

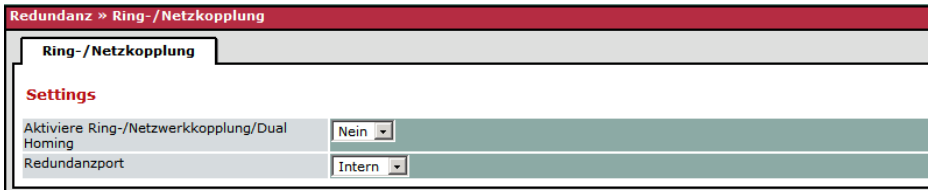
Geben Sie die IP-Adresse an.
Die Hosts müssen so konfiguriert sein, dass sie ICMP Echo Requests beantworten.

Zu überprüfende Hosts im internen Netzwerk

Geben Sie die IP-Adresse an.
Die Hosts müssen so konfiguriert sein, dass sie ICMP Echo Requests beantworten.

6.12.2 Ring-/Netzkopplung

Ring-/Netzkopplung



Settings

Aktiviere Ring-/Netzkopplung/Dual Homing: Ja / Nein

Bei Aktivierung wird im Stealth-Modus der Status der Ethernetverbindung von einen Port auf den anderen übertragen, wodurch sich Unterbrechungen im Netzwerk leicht zurückverfolgen lassen.

Redundanzport: Intern / Extern

Intern: Wenn die Verbindung am LAN-Port wegfällt/kommt, wird auch der WAN-Port ausgeschaltet/eingeschaltet.

Extern: Wenn die Verbindung am WAN-Port wegfällt/kommt, wird auch der LAN-Port ausgeschaltet/eingeschaltet.

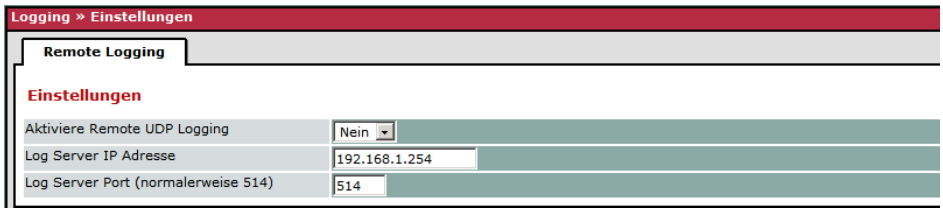
6.13 Menü Logging

Unter Logging versteht man die Protokollierung von Ereignismeldungen z. B. über vorgenommene Einstellungen, über Greifen von Firewall-Regeln, über Fehler usw.

Log-Einträge werden unter verschiedenen Kategorien erfasst und können nach Kategorie sortiert angezeigt werden - siehe „Logging » Logs ansehen“ auf Seite 256.

6.13.1 Logging » Einstellungen

Remote Logging



Alle Log-Einträge finden standardmäßig im Arbeitsspeicher des mGuard statt. Ist der maximale Speicherplatz für diese Protokollierungen erschöpft, werden automatisch die ältesten Log-Einträge durch neue überschrieben. Zudem werden beim Ausschalten des mGuard alle Log-Einträge gelöscht.

Um das zu verhindern, ist es möglich, die Log-Einträge (SysLog-Meldungen) auf einen externen Rechner (SysLog-Server) zu übertragen. Das liegt auch dann nahe, sollte eine zentrale Verwaltung der Protokollierungen mehrerer mGuards erfolgen.

Einstellungen

Aktiviere Remote UDP Logging: Ja / Nein

Sollen alle Log-Einträge zum externen (unten angegebenen) Log Server übertragen werden, setzen Sie diesen Schalter auf **Ja**.

Log Server IP Adresse

Geben Sie die IP-Adresse des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen.

☞ Sie müssen eine IP-Adresse angeben, keinen Hostnamen! Hier wird eine Namensauflösung nicht unterstützt, weil sonst bei Ausfall eines DNS-Servers unter Umständen nicht protokolliert werden könnte.

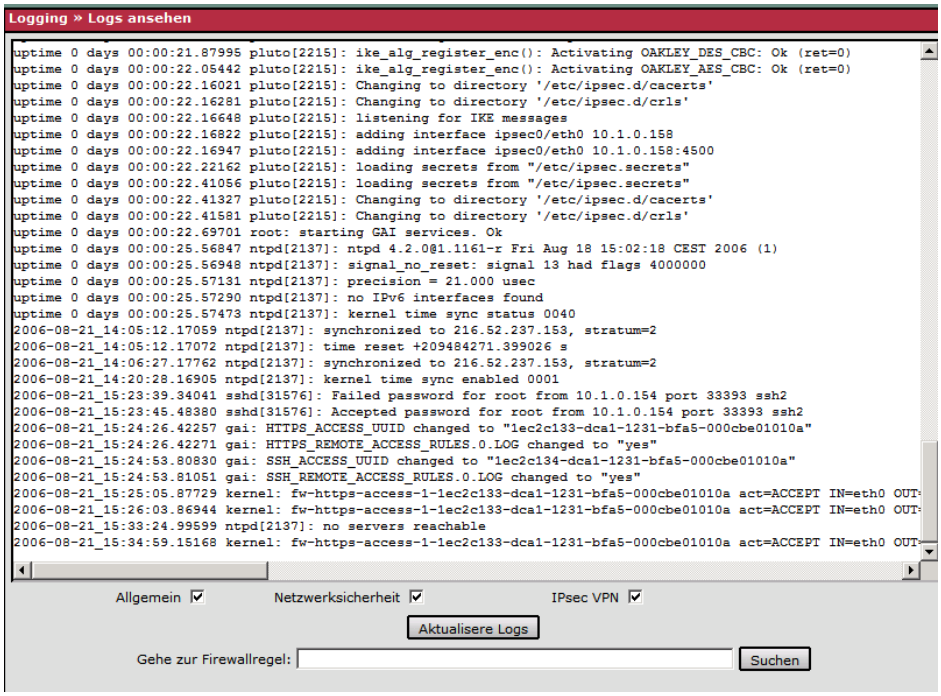
Log Server Port (normalerweise 514)

Geben Sie den Port des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Standard: 514

⌦ Sollen SysLog-Meldungen über einen VPN-Kanal auf einen SysLog-Server übertragen werden, dann muss sich die IP-Adresse des SysLog-Servers in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote**-Netzwerk angegeben ist. Und die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Lokal** angegeben ist (siehe „VPN-Verbindung / VPN-Verbindungskanäle definieren“ auf Seite 214).

– Ist dabei die Option **Aktiviere 1-zu-1-NAT des lokalen Netzwerkes in ein internes Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 220), gilt Folgendes: Die interne IP-Adresse (im Stealth-Modus die **Stealth Management IP-Adresse** bzw. **Virtuelle IP**) muss sich in dem Netzwerk befinden, das mit **Interne Netzwerkadresse für lokales 1-zu-1-NAT** angegeben ist.
– Ist dabei die Option **Aktiviere 1-zu-1-NAT des gegenüberliegenden Netzwerkes auf ein anders Netz** auf **Ja** gestellt (siehe „1-zu-1-NAT“ auf Seite 220), gilt Folgendes: Die IP-Adresse des SysLog-Servers muss sich in dem Netzwerk befinden, das in der Definition der VPN-Verbindung als **Remote** angegeben ist.

6.13.2 Logging » Logs ansehen


Logging » Logs ansehen
uptime 0 days 00:00:21.87995 pluto[2215]: ike_alg_register_enc(): Activating OAKLEY_DES_CBC: Ok (ret=0)
uptime 0 days 00:00:22.05442 pluto[2215]: ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok (ret=0)
uptime 0 days 00:00:22.16021 pluto[2215]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:22.16281 pluto[2215]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:22.16648 pluto[2215]: listening for IKE messages
uptime 0 days 00:00:22.16822 pluto[2215]: adding interface ipsec0/eth0 10.1.0.158
uptime 0 days 00:00:22.16947 pluto[2215]: adding interface ipsec0/eth0 10.1.0.158:4500
uptime 0 days 00:00:22.22162 pluto[2215]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:22.41056 pluto[2215]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:22.41327 pluto[2215]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:22.41581 pluto[2215]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:22.69701 root: starting GAI services. Ok
uptime 0 days 00:00:25.56847 ntpd[2137]: ntpd 4.2.0@1.1161-r Fri Aug 18 15:02:18 CEST 2006 (1)
uptime 0 days 00:00:25.56948 ntpd[2137]: signal_no_reset: signal 13 had flags 4000000
uptime 0 days 00:00:25.57131 ntpd[2137]: precision = 21.000 usec
uptime 0 days 00:00:25.57290 ntpd[2137]: no IPv6 interfaces found
uptime 0 days 00:00:25.57473 ntpd[2137]: kernel time sync status 0040
2006-08-21_14:05:12.17059 ntpd[2137]: synchronized to 216.52.237.153, stratum=2
2006-08-21_14:05:12.17072 ntpd[2137]: time reset +209484271.399026 s
2006-08-21_14:06:27.17762 ntpd[2137]: synchronized to 216.52.237.153, stratum=2
2006-08-21_14:20:28.16905 ntpd[2137]: kernel time sync enabled 0001
2006-08-21_15:23:39.34041 sshd[31576]: Failed password for root from 10.1.0.154 port 33393 ssh2
2006-08-21_15:23:45.48380 sshd[31576]: Accepted password for root from 10.1.0.154 port 33393 ssh2
2006-08-21_15:24:26.42257 gai: HTTPS_ACCESS_UUID changed to "1ec2c133-dca1-1231-bfa5-000cbe01010a"
2006-08-21_15:24:26.42271 gai: HTTPS_REMOTE_ACCESS_RULES.0.LOG changed to "yes"
2006-08-21_15:24:53.80830 gai: SSH_ACCESS_UUID changed to "1ec2c134-dca1-1231-bfa5-000cbe01010a"
2006-08-21_15:24:53.81051 gai: SSH_REMOTE_ACCESS_RULES.0.LOG changed to "yes"
2006-08-21_15:25:05.87729 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
2006-08-21_15:26:03.86944 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
2006-08-21_15:33:24.99599 ntpd[2137]: no servers reachable
2006-08-21_15:34:59.15168 kernel: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a act=ACCEPT IN=eth0 OUT
Allgemein
Netzwerksicherheit
IPsec VPN
Aktualisere Logs
Gehe zur Firewallregel:
Suchen

Je nachdem, welche Funktionen des mGuard aktiv gewesen sind, werden unterhalb der Log-Einträge entsprechende Kontrollkästchen zum Filtern der Einträge nach Kategorien angezeigt.

Damit eine oder mehrerer Kategorien angezeigt werden, aktivieren Sie das/die Kontrollkästchen der gewünschten Kategorie(n) und klicken dann auf die Schaltfläche **Aktualisiere Logs**.

Kategorien der Log-Einträge

Allgemein

Log-Einträge, die den anderen Kategorien nicht zugeordnet werden können.

Netzwerksicherheit

Ist bei Festlegung von Firewall-Regeln das Protokollieren von Ereignissen festgelegt (Log = Ja), dann können Sie hier das Log aller protokollierten Ereignisse einsehen.

Log ID und Nummer zum Auffinden von Fehlerquellen

Log-Einträge, die sich auf die nachfolgend aufgelisteten Firewall-Regeln beziehen, haben eine Log ID und eine Nummer. Anhand dieser Log ID und Nr. ist es möglich, die Firewall-Regel ausfindig zu machen, auf die sich der betreffende Log-Eintrag bezieht und die zum entsprechenden Ereignis geführt hat.

Firewall-Regeln und ihre Log ID

- Paketfilter:
  Menü Netzwerksicherheit » Paketfilter » Eingangsregeln / Ausgangsregeln
  Log ID: **`fw-incoming`** bzw. **`fw-outgoing`**
- Firewall-Regeln bei VPN-Verbindungen:
  Menü IPsec VPN » Verbindungen » Firewall eingehend / ausgehend
  Log ID: **`vpn-fw-in`** bzw. **`vpn-fw-out`**
- Firewall-Regeln bei Web-Zugriff auf den mGuard über HTTPS:

Menü Verwaltung » Web-Einstellungen » Zugriff
Log ID: **fw-https-access**

- Firewall-Regeln bei Zugriff auf den mGuard über SNMP:
  Menü Verwaltung » SNMP » Abfrage
  Log ID: **fw-snmp-access**
- Firewall-Regeln bei SSH Fernzugriff auf den mGuard:
  Menü Verwaltung » Systemeinstellungen » Shell Zugang
  Log ID: **fw-ssh-access**
- Firewall-Regeln der Benutzerfirewall:
  Menü Netzwerksicherheit » Benutzerfirewall » Firewall-Regeln
  Log ID: **ufw-**
- Regeln für NAT, Port-Weiterleitung
  Menü Netzwerk » NAT » Portweiterleitung

  Log ID: **fw-portforwarding**
- Firewall-Regeln für serielle Schnittstelle:
  Menü Netzwerk » Interfaces » Serielle Schnittstelle
  Eingangsregeln
  Log ID: **fw-serial-incoming**

  Ausgangsregeln

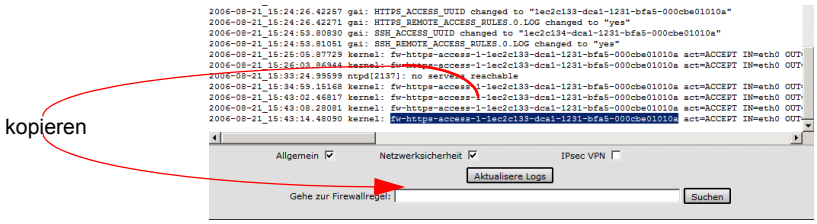
  Log ID: **fw-serial-outgoing**

Suche nach Firewall-Regel auf Grundlage eines Netzwerksicherheits-Logs

Ist das Kontrollkästchen **Netzwerksicherheit** aktiviert, sodass die betreffenden Log-Einträge angezeigt werden, wird unterhalb der Schaltfläche *Aktualisiere Logs* das Suchfeld **Gehe zur Firewallregel** angezeigt.

Gehen Sie wie folgt vor, wenn Sie die Firewall-Regel ausfindig machen wollen, auf die sich ein Log-Eintrag der Kategorie *Netzwerksicherheit* bezieht und die zum entsprechenden Ereignis geführt hat:

1. Beim betreffenden Log-Eintrag die Passage markieren, die die Log-ID und Nummer enthält, z. B.: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a



2. Diese Passage über die Zwischenablage ins Feld **Gehe zur Firewallregel** kopieren.
3. Auf die Schaltfläche **Suchen** klicken.
   Folge:

   Es wird die Konfigurationsseite mit der Firewall-Regel angezeigt, auf die sich der Log-Eintrag bezieht.

Blade

Auf dem Bladekontroller werden, neben Fehlermeldungen, die folgenden Meldungen ausgegeben:

(Die mit < und > umklammerten Bereiche sind in den Log-Einträgen durch die

jeweiligen Daten ersetzt.)

Allgemeine Meldungen:

```
blade daemon "<version>" starting ...
Blade[<bladenr>] online
Blade[<bladenr>] is mute
Blade[<bladenr>] not running
Reading timestamp from blade[<bladenr>]
```

Beim Aktivieren eines Konfigurationsprofils auf einem Blade:

```
Push configuration to blade[<bladenr>]
reconfiguration of blade[<bladenr>] returned <returncode>
blade[<bladenr>] # <text>
```

Beim Holen eines Konfigurationsprofils vom Blade:

```
Pull configuration from blade[<bladenr>]
Pull configuration from blade[<bladenr>] returned <returncode>
```

Anti-Virus

Das Virus-Log enthält folgende Meldungen des Virenfilters:

- Gefundene Viren mit Angabe von Details (Name des Virus, Name der Datei, bei einer E-Mail zusätzlich: Absender, Datum, Betreff)
- Ausgegebene Warnungen bei automatischer Einschaltung des Durchlassmodus, wenn die zu filternde Datei die eingestellte Dateigröße überschreitet und nicht gefiltert wurde.
- Start und Ende der Virenfilterprogramme.
- Fehlerausgaben des Virenfilters

Fehlermeldungen:

Virus Detection

Ein Virus wurde erkannt. Die Fehlermeldung enthält den Namen des Virus, den Absender der E-Mail, das Absendedatum und den Namen der infizierten Datei bzw. den Namen der komprimierten Archivdatei und des infizierten Bestandteils dieses Archivs.

Beispiel einer Virenmeldung:

```
mGuard detected a virus. The mail could not be delivered.
found Virus Email-Worm.Win32.NetSky.q /[From
sick@example.com][Date Fri, 13 Aug 2004 11:33:53++0200]/
about_you.zip/document.txt.exe
[000012a7.00000077.00000000]
Message Details:
From: sick@example.com
Subject: Private document
Date: Fri, 13 Aug 2004 11:33:53 +0200
```

Exceeded maximum filesize

Die eingestellte Begrenzung der Dateigröße wurde überschritten.

Um die Datei trotzdem übertragen zu können, deaktivieren Sie für den Download den Virenfilter für den entsprechenden Server oder global. Alternativ können Sie unter Menü *Web-Sicherheit* bzw. *E-Mail-Sicherheit* den Einstellparameter „bei Überschreiten der Größenbegrenzung“ auf den Durchlassmodus schalten.

⌦ In beiden Fällen wird die übertragene Datei nicht nach Viren untersucht!

Temporary Virus Scanner Failure

Ein temporärer Fehler trat bei dem Versuch auf, eine Datei zu scannen. Eine Wiederholung der Übertragung zu einem späteren Zeitpunkt oder ein Update der Virensignaturdatei kann evtl. das Problem beheben.

Mögliche Fehlerursachen:

- Die Scan-Engine ist nicht in der Lage, die Datei zu bearbeiten
- Die Speicherkapazität des Innominate mGuard reicht nicht zur Dekompression der Datei aus
- Interner Fehler der Scan-Engine

Exceptional Virus Scanner Failure

Ein Kommunikationproblem mit der Scan-Engine trat auf.

Mögliche Fehlerursachen:

- Fehlgeschlagenes Signatur-Update durch fehlerhafte Angabe des Update-Servers (Menüpunkt Verwaltung -> Update)
- Ungültige Lizenz für den Virenfilter
- Beschädigtes oder fehlerhaftes Update der Virensignaturdatei

Update running

Der Virenfilter verfügt über keine Virensignaturen, der Download der Virensignaturen wurde bereits gestartet. Sie können den Fortschritt des Downloads im Menüpunkt Logging -> Logs ansehen -> Anti-Virus Update verfolgen.

DHCP Server/Relay

Meldungen der unter Netzwerk -> DHCP konfigurierbaren Dienste.

Anti-Virus Update

Das Update-Log enthält Meldungen über den Start und Verlauf des Update-Prozesses der Virensignaturdateien.

SNMP/LLDP

Meldungen der unter Verwaltung -> SNMP konfigurierbaren Dienste.

IPsec VPN

Listet alle VPN-Ereignisse auf.

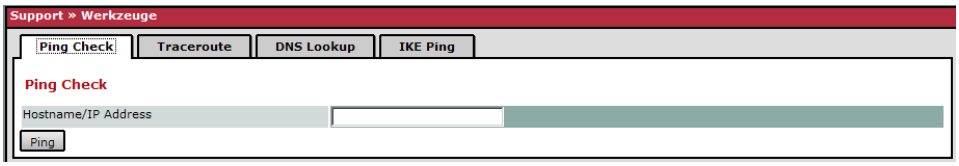
Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

6.14 Menü Support

6.14.1 Support » Werkzeuge

Ping Check



Ping Check

Ziel:

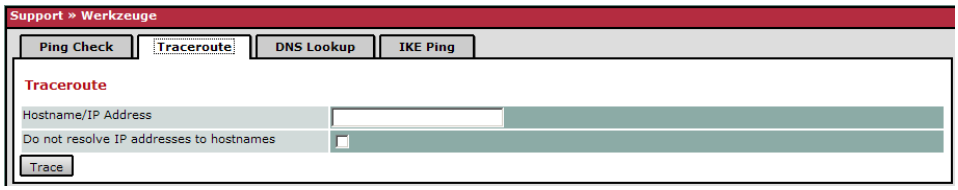
Sie wollen überprüfen, ob eine Gegenstelle über ein Netzwerk erreichbar ist.

Vorgehen:

In das Feld **Hostname/IP-Adresse** die IP-Adresse oder den Hostnamen der Gegenstelle eingeben. Dann auf die Schaltfläche **Ping** klicken.

Sie erhalten daraufhin eine entsprechende Meldung.

Traceroute



Traceroute

Ziel:

Sie wollen wissen, welche Zwischenstellen oder Router sich auf dem Verbindungsweg zu einer Gegenstelle befinden.

Vorgehen:

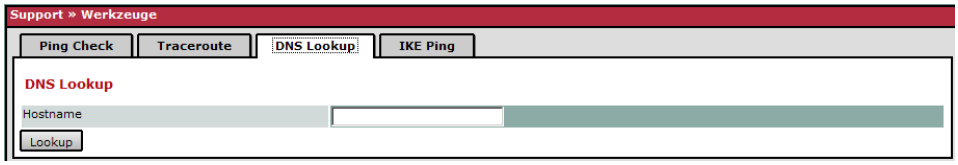
In das Feld **Hostname/IP Address** den Hostnamen oder IP-Adresse der Gegenstelle eintragen, zu der die Route ermittelt werden soll.

Falls die auf der Route gelegenen Stellen mit IP-Adresse statt mit Hostnamen (falls vorhanden) ausgegeben werden sollen, aktivieren Sie das Kontrollkästchen **Do not resolve IP addresses to hostnames** (= Häkchen setzen).

Dann auf die Schaltfläche **Trace** klicken.

Sie erhalten daraufhin eine entsprechende Meldung.

DNS Lookup



DNS Lookup

Ziel:

Sie wollen wissen,

welcher Hostname zu einer bestimmten IP-Adresse gehört
ODER

welche IP-Adresse zu einem bestimmten Hostnamen gehört.

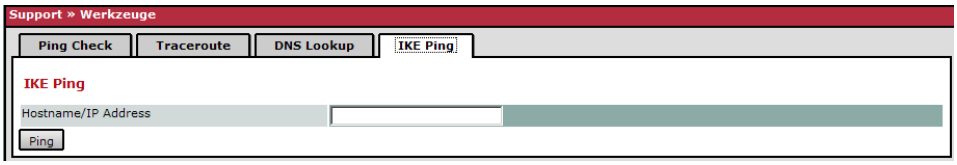
Vorgehen:

In das Feld **Hostname** die IP-Adresse bzw. den Hostnamen eingeben.

Auf die Schaltfläche **Lookup** klicken.

Sie erhalten daraufhin die Antwort, wie sie der mGuard aufgrund seiner DNS-Konfiguration ermittelt.

IKE Ping



IKE Ping

Ziel:

Sie wollen ermitteln, ob die VPN-Software eines VPN-Gateways in der Lage ist, eine VPN-Verbindung aufzubauen, oder ob z. B. eine Firewall das verhindert.

Vorgehen:

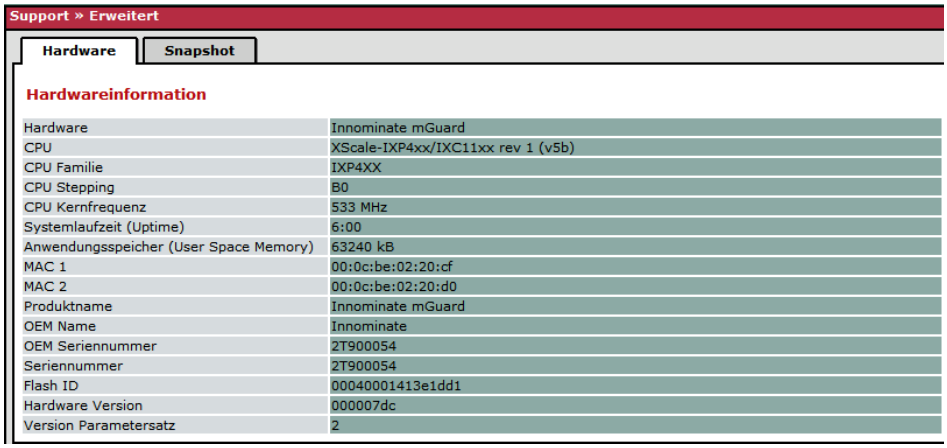
In das Feld **Hostname/IP Address** den Namen bzw. die IP-Adresse des VPN-Gateways eingeben.

Auf die Schaltfläche **Ping** klicken.

Sie erhalten eine entsprechende Meldung.

6.14.2 Support » Erweitert

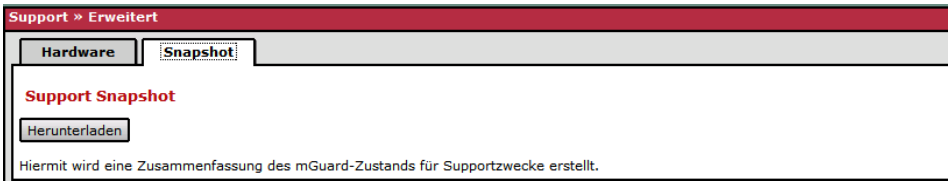
Hardware



Hardware	Innominate mGuard
CPU	XScale-IXP4xx/IXC11xx rev 1 (v5b)
CPU Familie	IXP4XX
CPU Stepping	B0
CPU Kernfrequenz	533 MHz
Systemlaufzeit (Uptime)	6:00
Anwendungsspeicher (User Space Memory)	63240 kB
MAC 1	00:0c:be:02:20:cf
MAC 2	00:0c:be:02:20:d0
Produktname	Innominate mGuard
OEM Name	Innominate
OEM Seriennummer	2T900054
Seriennummer	2T900054
Flash ID	00040001413e1dd1
Hardware Version	000007dc
Version Parametersatz	2

Diese Seite listet verschiedene Hardwareeigenschaften des mGuards auf.

Snapshot



Diese Funktion dient für Support-Zwecke.

Erstellt eine komprimierte Datei (im tar.gz-Format), in der alle aktuellen Konfigurations-Einstellungen und Log-Einträge erfasst sind, die zur Fehlerdiagnose relevant sein könnten.

⌦ Diese Datei enthält keine privaten Informationen wie z. B. private Maschinenzertifikate oder Passwörter. Eventuell benutzte Pre-Shared Keys von VPN-Verbindungen sind jedoch in Snapshots enthalten.

Um einen Snapshot zu erstellen, gehen Sie wie folgt vor:

1. Die Schaltfläche **Herunterladen** klicken.
2. Die Datei speichern (unter dem Namen snapshot.tar.gz)

Stellen Sie die Datei dem Support zur Verfügung, wenn dies erforderlich ist.

6.15 CIDR (Classless Inter-Domain Routing)

IP Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinanander folgenden Adressen als ein Netzwerk behandelt.

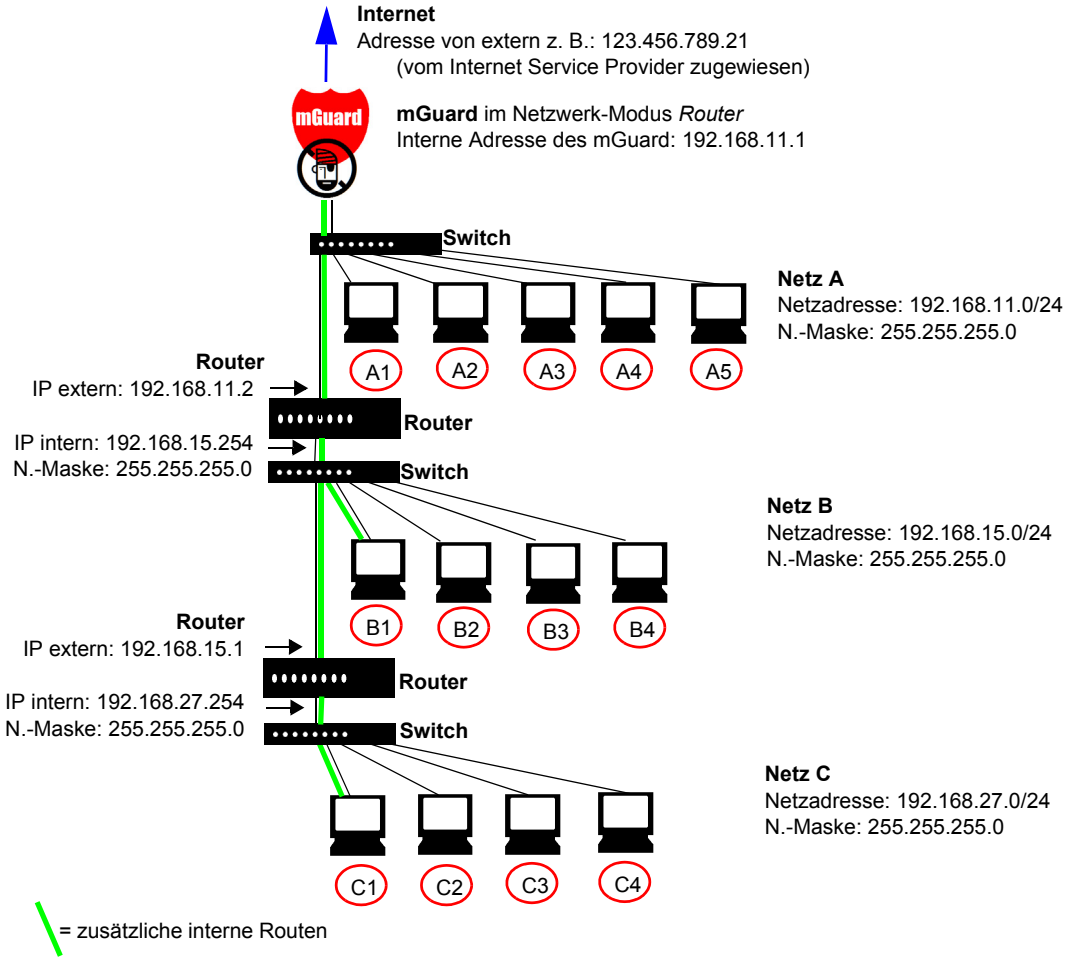
Um dem mGuard einen Bereich von IP-Adressen anzugeben, z. B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

6.16 Netzwerk-Beispielskizze

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie beim mGuard die Angaben zusätzlicher interner Route lauten könnten.



Netz A

Rechner	A1	A2	A3	A4	A5
IP-Adresse	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz B

Rechner	B1	B2	B3	B4
IP-Adresse	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz C

Rechner	C1	C2	C3	C4
IP-Adresse	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Zusätzliche interne Routen:
Netzwerk: 192.168.15.0/24
Gateway: 192.168.11.2

Netzwerk: 192.168.27.0/24
Gateway: 192.168.11.2

7 Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware

Die Rescue-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

7.1 Neustart durchführen

Ziel Das Gerät neu starten mit den konfigurierten Einstellungen.

Aktion: **Rescue-Taste** für ca. 1,5 Sekunden drücken:

- mGuard industrial RS: bis die "Error" LED leuchtet
- smart: Bis die mittlere LED in Rot aufleuchtet.
- blade, PCI: bis beide roten LEDs aufleuchten
- EAGLE mGuard: bis die Status LED und die Link-LEDs aufhören zu leuchten
- delta: bis die Status LED aufhört zu blinken

ODER

- Die Stromzufuhr vorübergehend unterbrechen.
- mGuard PCI: Den Computer, welcher die mGuard PCI Karte enthält, neu starten.

7.2 Recovery-Prozedur ausführen

Ziel Weil auf den mGuard nicht mehr zugegriffen werden kann, soll die Netzwerkkonfiguration in den Auslieferungszustand zurückgesetzt werden:
Alle mGuard-Versionen bis auf mGuard delta und blade Kontroller in den *Stealth*-Modus (automatisch) mit der Adresse 1.1.1.1 mGuard delta und beim blade Kontroller in den *Router*-Modus mit der Adresse 192.168.1.1.

Weiterhin wird für die Ethernetanschlüsse das MAU Management eingeschaltet, HTTPS über den lokalen Ethernetanschluß (LAN) freigegeben.

⌦ Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:
Der mGuard befindet sich im Router- oder PPPoE-Modus und
– die Geräteadresse des mGuard ist konfiguriert worden abweichend von der Standardeinstellung und
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktion:

1. Die **Rescue-Taste** langsam 6-mal drücken.
2. Nach ca. 2 Sekunden antwortet der mGuard:

- mGuard industrial RS
  - Bei Erfolg leuchtet die „State“ LED grün
  - Bei Misserfolg leuchtet die „Error“ LED rot
- smart
  - Bei Erfolg leuchtet die mittlere LED grün
  - Bei Misserfolg leuchtet die mittlere LED rot
- blade, PCI
  - Bei Erfolg leuchtet die LAN LED rot
  - Bei Misserfolg leuchtet die WAN LED rot
- EAGLE mGuard
  - Bei Erfolg leuchtet die STATUS LED gelb
  - Bei Misserfolg leuchtet die ERROR LED rot
- mGuard delta
  - Bei Erfolg leuchtet die STATUS LED grün
  - Bei Misserfolg bleibt die Status LED aus.

3. Drücken Sie anschließend erneut die **Resuce-Taste** langsam 6-mal.
4. Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den *Stealth*-Modus (mGuard delta und blade Kontroller: Router-Modus). Es ist dann wieder unter folgender Adresse zu erreichen: **https://1.1.1.1/** (mGuard delta und blade Kontroller: https://192.168.1.1/)

7.3 Flashen der Firmware

Ziel Die gesamte Software des mGuard soll neu ins Gerät geladen werden.

⌦ **Alle konfigurierten Einstellungen werden gelöscht.** Der mGuard wird in den Auslieferungszustand versetzt.
Ab Version 5.0.0 des mGuard bleiben die im mGuard installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

⌦ Beim mGuard industrial RS ist nur die Firmware ab Version 5.1.0 installierbar.

Mögliche Gründe zum Flashen der Firmware:

- Das Administrator- und Root-Passwort sind verloren gegangen.

Aktion: Gehen Sie wie folgt vor:

⌦ **Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des mGuard unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.**

Voraussetzungen:

- Sie haben die Software des mGuard vom Innominate-Support oder von der Web-Site www.innominate.com bezogen und auf dem Konfigurations-Rechner gespeichert.
- Falls die Ihnen vorliegende Software-Version höher ist als die beim Ausliefe-

rungszustand des Gerätes, müssen Sie eine Lizenz für die Nutzung dieses Updates erwerben. Das gilt für Major-Release Upgrades, also z. B. bei Upgrade von Version 4.x.y zu Version 5.x.y zu Version 6.x.y usw.

- DHCP- und TFTP-Server sind unter der gleiche IP Adresse zu erreichen - siehe „Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server" auf Seite 268.
- mGuard PCI: Wird der mGuard im Power-over-PCI Modus betrieben, muss der DHCP/TFTP Server über die LAN Buchse des mGuard angeschlossen sein. Wird der mGuard im PCI Treibermodus betrieben, muss der DHCP/TFTP Server auf dem Rechner bzw. unter dem Betriebssystem ausgeführt werden, das die Schnittstelle zum mGuard bereitstellt.

1. **Rescue-Taste** gedrückt halten, bis der *Recovery-Status* wie folgt eintritt:

   Der mGuard wird neu gestartet (nach ca. 1,5 Sekunden), nach weiteren ca. 1,5 Sekunden gelangt der mGuard in den *Recovery-Status*:
   - mGuard industrial RS: die LEDs "State", "LAN" und "WAN" leuchten grün
   - smart: alle LEDs leuchten grün
   - blade, PCI: die grünen sowie die rote LAN LED leuchten
   - EAGLE mGuard: die LEDs 1, 2 und V.24 leuchten
   - delta: die Status LED wird langsam dunkel

2. Spätestens 1 Sekunde nach Eintritt des *Recovery-Status* die **Rescue-Taste** loslassen. (Falls Sie die **Rescue-Taste** nicht loslassen, wird der mGuard neu gestartet.)
   Der mGuard startet nun das Recovery-System: Er sucht über die LAN Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

- Statusanzeige:
  - mGuard industrial RS: die „State" LED blinkt
  - smart: die mittlere LED (Heartbeat) blinkt
  - blade, PCI: die rote LAN LED blinkt
  - EAGLE mGuard: die LEDs 1, 2 und V.24 leuchten orange auf
  - delta: die Status LED blinkt

  Vom TFTP-Server wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur von Innominate unterschriebene Dateien werden ausgeführt.
  Die Kontrollprozedur löscht nun den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Software vor.
- Statusanzeige:
  - mGuard industrial RS: die LEDs "Modem", "State" und "LAN" bilden ein Lauflicht
  - smart: die 3 grünen LEDs bilden ein Lauflicht
  - blade, PCI: die grünen und die rote LAN LED bilden ein Lauflicht
  - EAGLE mGuard: die LEDs 1, 2 und V.24 bilden ein Lauflicht
  - delta: die Status LED blinkt schneller

  Vom TFTP-Server wird die Software jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Innominate signierte Dateien werden akzeptiert.
  Dieser Vorgang dauert ca. 3 bis 5 Minuten.

- Statusanzeige:
  - mGuard industrial RS: die „State“ LED leuchtet kontinuierlich
  - smart: Die mittlere LED (Heartbeart) leuchtet kontinuierlich.
  - blade, PCI: blinken die grünen LEDs und die rote LAN LED gleichzeitig durchgehend
  - EAGLE mGuard: die LEDs 1, 2 und V.24 sind aus, die LEDs p1, p2 und Status leuchten kontinuierlich grün
  - delta: die Status LED leuchtet kontinuierlich

  Die neue Software wird entpackt und konfiguriert. Das dauert ca. 20 Minuten.

  Sobald die Prozedur beendet ist, geschieht Folgendes:
  - mGuard industrial RS: Die LEDs "Modem", "State" und "LAN" blinken gleichzeitig grün.
  - smart: Alle 3 LEDs blinken gleichzeitig grün.
  - blade, PCI:
    PCI - Der mGuard startet neu.
    blade - Die LEDs WAN grün, LAN grün und WAN rot blinken gleichzeitig.
  - EAGLE mGuard: Die LEDs 1, 2 und V.24 blinken gleichzeitig grün.
  - delta: Die Status LED blinkt einmal pro Sekunde.

3. Starten Sie den mGuard neu. Dies ist beim mGuard blade und PCI nicht erforderlich.
   Drücken Sie dazu kurz die **Rescue-Taste**.
   ODER
   Unterbrechen Sie seine Stromversorgung und schließen Sie ihn dann wieder an (smart: per USB-Kabel, das ausschließlich zur Stromversorgung dient).

   Folge:
   Der mGuard befindet sich im Auslieferungs-Zustand. Konfigurieren Sie ihn neu - siehe „Lokale Konfigurationsverbindung herstellen” auf Seite 53.

Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server

Zum „Flashen“ der Firmware muss auf dem lokal angeschlossenen Rechner ein DHCP- und TFTP-Server installiert sein.
(DHCP = **D**ynamic **H**ost **C**onfiguration **P**rotocol; TFTP = **T**rivial **F**ile **T**ransfer **P**rotocol)

Installieren Sie den DHCP- und TFTP-Server, falls notwendig (siehe unten).

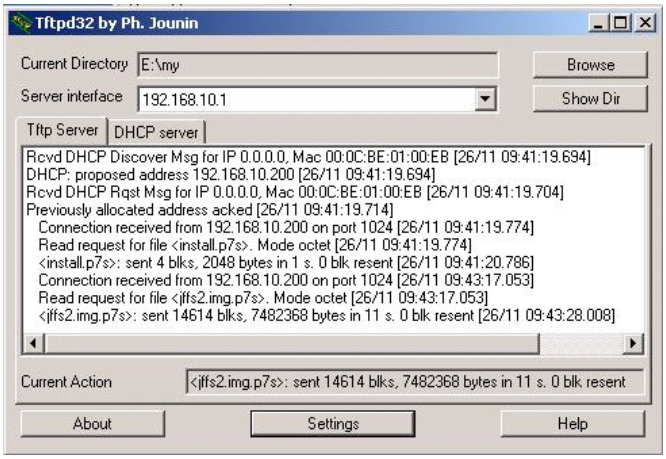
⌦ Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden!

7.3.1 DHCP- und TFTP-Server unter Windows oder Linux installieren

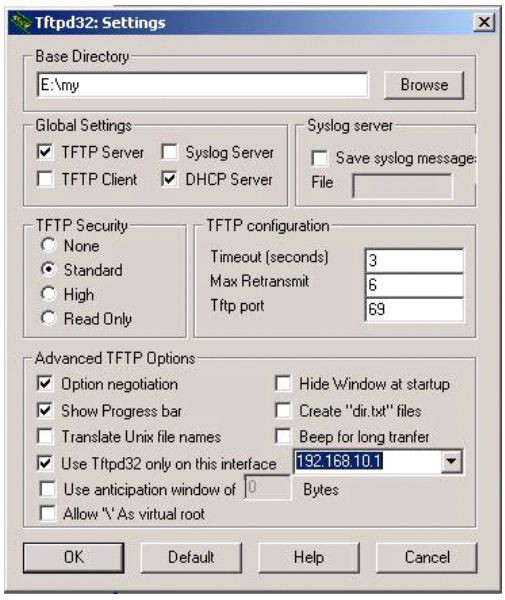
Unter Windows

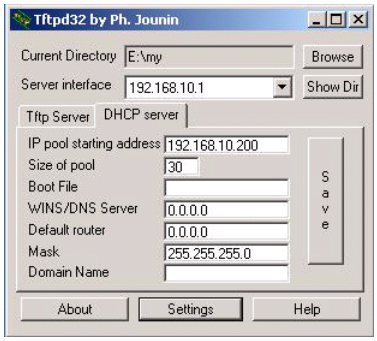
Installieren Sie das Programm, welches im Download-Bereich von Innominates Web-Site www.innominate.de zu finden ist. Gehen Sie dazu wie folgt vor:

1. Ist der Windows-Rechner an einem Netzwerk angeschlossen, trennen Sie ihn von diesem.
2. Kopieren Sie die Software in einen beliebigen leeren Ordner des Windows-Rechners. Starten Sie das Programm TFTPD32.EXE
3. Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.
   Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die mGuard-Imagedateien gespeichert sind: **install.p7s, jffs2.img.p7s**
   Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** ebenfalls dort abgelegt werden. Bitte stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört. (Siehe „Verwaltung » Update" auf Seite 85).


Tftpd32 by Ph. Jounin
Current Directory E:\my
Browse
Server interface 192.168.10.1
Show Dir
Tftp Server
DHCP server
Rcvd DHCP Discover Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.694]
DHCP: proposed address 192.168.10.200 [26/11 09:41:19.694]
Rcvd DHCP Rqst Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.704]
Previously allocated address acked [26/11 09:41:19.714]
Connection received from 192.168.10.200 on port 1024 [26/11 09:41:19.774]
Read request for file <install.p7s>. Mode octet [26/11 09:41:19.774]
<install.p7s>: sent 4 blks, 2048 bytes in 1 s. 0 blk resent [26/11 09:41:20.786]
Connection received from 192.168.10.200 on port 1024 [26/11 09:43:17.053]
Read request for file <jffs2.img.p7s>. Mode octet [26/11 09:43:17.053]
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent [26/11 09:43:28.008]
Current Action
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent
About
Settings
Help

4. Wechseln Sie auf die Registerkarte *Tftp Server* bzw. *DHCP Server* und klicken Sie dann die Schaltfläche **Settings**, um im dann angezeigten Dialogfeld die Parameter wie folgt zu setzen:





Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server. Installieren Sie die entsprechenden Pakete gemäß der Anleitung der jeweiligen Distribution.
Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcpd.conf** folgende Einstellungen vornehmen:

```
subnet 192.168.134.0 netmask 255.255.255.0 {
range 192.168.134.100 192.168.134.119;
option routers 192.168.134.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.134.255;}
```

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert:
/etc/inetd.conf
Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

Im Verzeichnis **/tftpboot** müssen die mGuard-Imagedateien gespeichert sein:
install.p7s, jffs2.img.p7s

Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** ebenfalls dort abgelegt werden. Bitte stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört. (Siehe „Verwaltung » Update” auf Seite 85)

Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
Sollten Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich bitte in der entsprechenden Dokumentation.

8 Glossar

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.
Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, dass die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.
Assymetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwendige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Da es sich hierbei um den ersten standardisierten Verschlüsselungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.
DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.
3DES ist eine Variante von DES. Es arbeitet mit drei mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

AES

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese » symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit.
1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

CA-Zertifikat

Wie vertrauenswürdig ist ein CA-Zertifikat und die CA (Certificate Authority), die es ausgestellt hat? (→ X.509 Zertifikat) Ein CA-Zertifikat kann herangezogen werden, um ein Zertifikat zu überprüfen, das die Signatur dieser CA trägt. Diese Prüfung macht nur dann Sinn, wenn davon auszugehen ist, dass das CA-Zertifikat aus authentischer Quelle stammt, also selber echt ist. Wenn darüber Zweifel bestehen, kann das CA-Zertifikat selber überprüft werden. Wenn es sich um ein Sub-CA-Zertifikat handelt, also ein CA-Zertifikat ausgestellt von einer Sub-CA (Sub Certificate Authority) - was normalerweise der Fall ist -,

kann das CA-Zertifikat der übergeordneten CA benutzt werden, um das CA-Zertifikat der ihr untergeordneten Instanz zu überprüfen. Und gibt es für diese übergeordnete CA eine weitere CA, die ihr wiederum übergeordnet ist, kann deren CA-Zertifikat benutzt weren, um das CA-Zertifikat der ihr untergeordneten Instanz zu prüfen, usw. Diese Kette des Vertrauens setzt sich fort bis zur Wurzelinstanz, die Root-CA (Root Certificate Authority). Die CA-Datei der Root-CA ist zwangsläufig selbst signiert. Denn diese Instanz ist die höchste, und der „Anker des Vertrauens“ liegt letztlich bei ihr. Es ist niemand mehr da, der dieser Instanz bescheinigen kann, dass sie die Instanz ist, für die sie sich ausgibt. Eine Root-CA ist daher eine staatliche oder staatlich kontrollierte Organisation.
Der mGuard kann die in ihn importierten CA-Zertifikate benutzen, um die von Gegenstellen „vorgezeigten“ Zertifikate auf Echtheit zu überprüfen. Bei VPN-Verbindungen z. B. kann die Authentifizierung der Gegenstelle ausschließlich durch CA-Zertifikate erfolgen. Dann müssen im mGuard alle CA-Zertifikate installiert sein, um mit dem von der Gegenstelle vorgezeigten Zertifikat eine Kette zu bilden: neben dem CA-Zertifikat der CA, deren Signatur im zu überprüfenden vorgezeigten Zertifikat des VPN-Partners steht, auch das CA-Zertifikat der ihr übergeordneten CA usw. bis hin zum Root-Zertifikat. Denn je lückenloser diese „Kette des Vertrauens“ überprüft wird, um eine Gegenstelle als authentisch zu akzeptieren, desto höher ist die Sicherheitsstufe.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.
Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D. h. der Client ist der anrufende Rechner, der Server (oder Host) der angerufene.

Datagramm

Bei IP Übertragungsprotokollen werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:

IP-Header	TCP, UDP, ESP etc. Header	Daten (Payload)

Der IP-Header enthält:
– die IP-Adresse des Absenders (source IP-address)
– die IP-Adresse des Empfängers (destination IP-address)
– die Protokollnummer des Protokolls der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
– die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:
– Port des Absenders (source port)
– Port des Empfängers (destination port)
– eine Prüfsume über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

Default Route

Ist ein Rechner an ein Netzwerk angeschlossen, erstellt das Betriebssystem intern eine Routing-Tabelle. Darin sind die IP-Adressen aufgelistet, die das Betriebssystem von den angeschlossenen Rechnern und den gerade verfügbaren Verbindungen (Routen) ermittelt hat. Die Routing-Tabelle enthält also die mögliche Routen (Ziele) für den Versand von IP-Paketen. Sind IP-Pakete zu verschicken, vergleicht das Betriebssystem des Rechners die in den IP-Paketen angegebenen IP-Adressen mit den Einträgen in der Routing-Tabelle, um die

richtige Route zu ermitteln.
Ist ein Router am Rechner angeschlossen und ist dessen interne IP-Adresse (d. h. die IP-Adresse des LAN Ports des Routers) als Standardgateway dem Betriebssystem mitgeteilt (bei der TCP/IP-Konfiguration der Netzwerkkarte), wird diese IP-Adresse als Ziel verwendet, wenn alle anderen IP-Adressen der Routing-Tabelle nicht passen. In diesem Fall bezeichnet die IP-Adresse des Routers die Default Route, weil alle IP-Pakete (per Default = standardmäßig) zu diesem Gateway geleitet werden, deren IP-Adressen in der Routing-Tabelle sonst keine Entsprechung, d. h. keine Route finden.

DynDNS-Anbieter

Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol). Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.
Soll ein solcher Rechner über das Internet erreichbar sein, muss er eine Adresse haben, die der entfernten Gegenstelle bekannt sein muss. Nur so kann diese die Verbindung zum Rechner aufbauen. Wenn die Adresse des Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des Rechners hat ein Account bei einem DynDNS-Anbieter (DNS = Domain Name Server). Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.example.com. Zudem stellt der DynDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.
Wenn jetzt ein entfernter Rechner eine Verbindung herstellen will zum Rechner, der beim DynDNS-Anbieter registriert ist, benutzt der entfernte Rechner den Hostnamen des Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurückübertragen zum entfernten Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten Rechner.
Allen Internetadressen liegt dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz, aufgebaut.

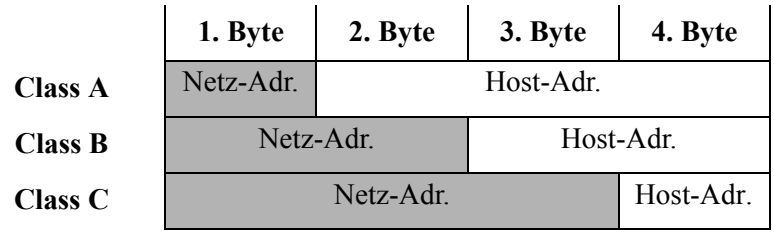
IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.
Eine IP-Adresse besteht aus 2 Teilen: die Netzwerk-Adresse und die Host-Adresse.

Netzwerk-Adresse	Host-Adresse

Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche

Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorie Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:



Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	Bytes für die Netzadresse	Bytes für die Host-Adresse
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

Subnetz-Maske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 123.456.789.21. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).
Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetz-Maske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu „borgen“, um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwendet werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

IPsec

IP Security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen (→ Datagramm) die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPsec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA) und der Internet Key Exchange (IKE).
Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. *Transport*

Mode oder *Tunnel Mode*
Im *Transport Mode* wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPsec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host- zu-Host-Verbindung geeignet.
Im *Tunnel Mode* wird dem gesamten IP-Datagramm ein IPsec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.
Der *Tunnel Mode* findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrekke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

Subject, Zertifikat

In einem Zertifikat werden von einer Zertifizierungsstelle (CA - Certificate Authority) die Zugehörigkeit des Zertifikats zu seinem Inhaber bestätigt. Das geschieht, indem bestimmte Eigenschaften des Inhabers bestätigt werden, ferner, dass der Inhaber des Zertifikats den privaten Schlüssel besitzt, der zum öffentlichen Schlüssel im Zertifikat passt. (→ X.509 Zertifikat).
Beispiel

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
    Validity
      Not Before: Oct 29 17:39:10 2000 GMT
→   Subject: CN=anywhere.com,E=doctrans.de,C=DE,ST=Hamburg,L=Hamburg,O=Innominate,OU=Security
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
          d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
          9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
          90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
          1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
          7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
          50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
          8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
          f0:b4:95:f5:f9:34:9f:f8:43
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        email:xyz@anywhere.com
      Netscape Comment:
        mod_ssl generated test server certificate
      Netscape Cert Type:
        SSL Server
  Signature Algorithm: md5WithRSAEncryption
    12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
    3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
    82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
    cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
    4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
    d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
    44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
    ff:8e
```

Der *Subject Distinguished Name*, kurz *Subject*, identifiziert den Zertifikatsinhaber eindeutig. Der Eintrag besteht aus mehreren Komponenten. Diese werden Attribute genannt - siehe das Beispiel-Zertifikat oben. Die folgende Tabelle listet die möglichen Attribute auf. In welcher Reihenfolge die Attribute in einem X.509-Zertifikat aufgeführt sind, ist unterschiedlich.

Abkürzung	Name	Erläuterung
CN	Common Name	Identifiziert die Person oder das Objekt, zu der/dem das Zertifikat gehört. Beipeil: CN=server1

Abkürzung	Name	Erläuterung
E	E-Mail-Adresse	Gibt die E-Mail-Adresse des Zertifikatsinhabers an.
OU	Organizational Unit	Gibt die Abteilung innerhalb einer Organisation oder Firma an. Beipiel: O=Entwicklung
O	Organization	Gibt die Organisation bzw. die Firma an. Beispiel: O=Innominate
L	Locality	Gibt den Ort an Beispiel: L=Hamburg
ST	State	Gibt den Bundesstaat bzw. das Bundesland an. Beispiel: ST=Bayern
C	Country	Code bestehend aus 2 Buchstaben, die das Land (= den Staat) angeben. (Deutschland = DE) Beispiel: C=DE

Bei VPN-Verbindungen sowie bei Fernwartungszugriffen auf den mGuard per SSH oder HTTPS kann für Subject (= Zertifikatsinhaber) ein Filter gesetzt werden. Dann werden nur solche Zertifikate von Gegenstellen akzeptiert, bei denen in der Zeile Subject bestimmte Attribute vorhanden sind.

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als *IP-Masquerading* bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt“. Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über die NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.

Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.

Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den UDP- bzw. TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzen Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.

Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Port-Nummer

Bei den Protokollen UDP und TCP wird jedem Teilnehmer eine Portnummer zugeordnet. Über sie ist es möglich zwischen zwei Rechnern mehrere UDP oder TCP Verbindungen zu unterscheiden und somit gleichzeitig zu nutzen.

Bestimmte Portnummern sind für spezielle Zwecke reserviert. Zum Beispiel werden in der Regel HTTP Verbindungen zu TCP Port 80 oder POP3 Verbindun-

gen zu TCP Port 110 aufgebaut.

Proxy

Ein Proxy (Stellvertreter) ist ein zwischengeschalteter Dienst. Ein Web-Proxy (z. B. Squid) wird gerne vor ein größeres Netzwerk geschaltet. Wenn z. B. 100 Mitarbeiter gehäuft auf eine bestimmte Webseite zugreifen und dabei über den Web-Proxy gehen, dann lädt der Proxy die entsprechenden Seiten nur einmal vom Server und teilt sie dann nach Bedarf an die anfragenden Mitarbeiter aus. Dadurch wird der Traffic nach außen reduziert, was Kosten spart.

PPPoE

Akronym für **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für **P**oint-to-**P**oint **T**unneling **P**rotocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll konzipiert, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

Router

Ein Router ist ein Gerät, das an unterschiedliche IP-Netze angeschlossen ist und zwischen diesen vermittelt. Dazu besitzt er für jedes an ihn angeschlossene Netz eine Schnittstelle (= Interface). Beim Eintreffen von Daten muss ein Router den richtigen Weg zum Ziel und damit die passende Schnittstelle bestimmen, über welche die Daten weiterzuleiten sind. Dazu bedient er sich einer lokal vorhandenen Routingtabelle, die angibt, über welchen Anschluss des Routers (bzw. welche Zwischenstation) welches Netzwerk erreichbar ist.

Trap

Vor allem in großen Netzwerken findet neben den anderen Protokollen zusätzlich das SNMP Protokoll (Simple Network Management Protocol) Verwendung. Dieses UDP-basierte Protokoll dient zur zentralen Administrierung von Netzwerkgeräten. Zum Beispiel kann man mit dem Befehl GET eine Konfigurationen abfragen, mit dem Befehl SET die Konfiguration eines Gerätes ändern, vorausgesetzt, das so angesprochene Netzwerkgerät ist SNMP-fähig.
Ein SNMP-fähiges Gerät kann zudem von sich aus SNMP-Nachrichten verschikken, z. B. wenn außergewöhnliche Ereignisse auftreten. Solche Nachrichten nennt man SNMP Traps.

X.509 Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.
Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.
Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguised Name (DN)), erlaubte Verwendungszwecke usw. und die Signatur der CA. (→ Subject, Zertifikat).
Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den

Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.
Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.
Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.
X.509 Zertifikate kommen z.B. bei Email Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Protokoll, Übertragungsprotokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutze Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Antispoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.
Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/ Internet Protocol)

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.
IP ist das Basisprotokoll.
UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.
TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.
UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.
Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).
ICMP baut auf IP auf und enthält Kontrollnachrichten.
SMTP ist ein auf TCP basierendes E-Mail-Protokoll.

IKE ist ein auf UDP basierendes IPsec-Protokoll.
ESP ist ein auf IP basierendes IPsec-Protokoll.
Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.
(→ Datagramm)

VLAN

Über ein VLAN (Virtual Local Area Network) kann man ein physikalisches Netzwerk logisch in getrennte, nebeneinander existierende Netze unterteilen. Die Geräte der unterschiedlichen VLANs können dabei nur Geräte in ihrem eigenen VLAN erreichen. Die Zuordnung zu einem VLAN wird damit nicht mehr nur allein von der Topologie des Netzes bestimmt, sondern auch durch die konfigurierte VLAN ID.

Die VLAN Einstellung kann als optionale Einstellung zu jeder IP vorgenommen werden. Ein VLAN wird dabei durch seine VLAN ID (1-4094) identifiziert. Alle Geräte mit der selben VLAN ID gehören dem gleichen VLAN an und können miteinander kommunizieren.
Das Ethernet-Paket wird für VLAN nach IEEE 802.1Q um 4 Byte erweitert, davon stehen 12 Bit zur Aufnahme der VLAN ID zur Verfügung. Die VLAN ID „0“ und „4095“ sind reserviert und nicht zur Identifikation eines VLANs nutzbar.

VPN (Virtuelles Privates Netzwerk)

Ein **V**irtuelles **P**rivates **N**etzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

9 Technische Daten

Allgemein

CPU	Intel IXP 42x mit 266 MHz bzw. 533 MHz
Speicher	16 MB Flash, 64 MB SDRAM; mGuard delta: 128 MB
LAN u. WAN Schnittstellen	Ethernet IEEE 802 10/100 Mbps RJ45
Seriell	RS 232
Stromversorgung	smart: Via USB-Schnittstelle (5 V, 500 mA) oder durch externes Netzteil (110 - 230 V) delta: 5VDC, 3A
Betriebssystem	Innominate Embedded Linux
Funktionsüberwachung	Watchdog und optische Anzeige
Relative Luftfeuchtigkeit	blade, smart, PCI: max. 90 % (nicht kondensierend) delta: 5-95% (nicht kondensierend)
Umgebungstemperatur	smart, blade, delta: 0-40°C PCI: 0-70°C

mGuard industrial RS

Netzausdehnung	Länge eines 10BASE-T/100BASE-TX Twisted Pair-Segmentes ca. 100 m
Betriebsspannung	9 bis 36 VDC; maximale transiente Überspannung 1500 V
Potentialdifferenz zwischen Eingangsspannung und Gehäuse	36 VDC
Leistungsaufnahme	maximal 4 W bei 24 VDC
Überstromschutz am Eingang	nicht wechselbare Schmelzsicherung
Abmessungen	45 mm x 100 mm x 111 mm (B x H x T)
Masse	250 g
Umgebungstemperatur	Umgebende Luft 0°C bis +55°C
Relative Luftfeuchtigkeit	10% bis 95% (nicht kondensierend)
Verschmutzungsgrad	2

EMV-Störfestigkeit	Entladung statischer Elektrizität Kontaktentladung: EN 61000-4-2 Luftentladung: EN 61000-4-2 Elektromagnetische Felder: EN 61000-4-3 Schnelle Transienten: EN 61000-4-4 Stoßspannungen symmetrisch: EN 61000-4-5 Stoßspannungen unsymmetrisch: EN 61000-4-5 Leitungsgebundene HF-Störungen: EN 61000-4-6 Alle Angaben jeweils ermittelt mit den Prüfschärfegraden, die gemäß EN 61131-2:2003 für Speicherprogrammierbare Steuerungen für den Einsatz in industriellen Umgebungen der Zone B erforderlich sind.
EMV-Störaussendung	EN 55022:2006: Class A CFR 47 FCC Part 15 (2005-4): Class A
Festigkeit	Schwingungsprüfung, sinusförmig nach EN 61131-2:2003 und DIN EN 60068-2-6:1996 (Prüfparameter gemäß Punkt 4.2.1 "Schwingungen" und Punkt 6.2.1 "Schwingungsprüfungen zu den normalen Betriebsbedingungen" der EN 61131-2:2003) Schockprüfung nach EN 61131-2:2003 und DIN EN 60068-2-27:1996 (Prüfparameter gemäß Punkt 4.2.2 "Schocken" und Punkt 6.2.2 "Schocks (Typprüfung zu den normalen Betriebsbedingungen)" der EN 61131-2:2003)
Zertifizierungen	CE, FCC

EAGLE mGuard

Netzausdehnung	Länge eines 10BASE-T/100BASE-TX Twisted Pair-Segmentes ca. 100 m
Betriebsspannung	NEC Class 2 power source 12VDC bzw. 9,6VDC - 60VDC oder 18VAC - 30 VAC Sicherheitskleinspannung (SELV/PELV, redundante Eingänge entkoppelt), max. 5A. Pufferzeit: min. 10 ms bei 24VDC
Potentialdifferenz zwischen Eingangsspannung und Gehäuse	Potentialdifferenz zu Eingangsspannung +24 VDC: 32 VDC Potentialdifferenz zu Eingangsspannung Masse: -32 VDC
Leistungsaufnahme	max. 7,2 W bei 24 VDC; 24,6 Btu (IT)/h
Überstromschutz am Eingang	nicht wechselbare Schmelzsicherung
Abmessungen	B x H x T 46 mm x 131 mm x 111 mm
Masse	340 g

Umgebungstemperatur	Umgebende Luft 0 ºC bis + 55 ºC
Lagerungstemperatur	Umgebende Luft - 40 ºC bis + 80 ºC
Relative Luftfeuchtigkeit	10% bis 95% (nicht kondensierend)
Luftdruck	geignet bis 2000 m (795 hPa)
Verschmutzungsgrad	2
EMV-Störfestigkeit	Entladung statischer Elektrizität Kontaktentladung: EN 61000-4-2 Prüfschärfegrad 3 Luftentladung: EN 61000-4-2 Prüfschärfegrad 3 Elektromagnetische Felder: EN 61000-4-3 Prüfschärfegrad 3 Schnelle Transienten: EN 61000-4-4 Prüfschärfegrad 3 Stoßspannungen symmetrisch: EN 61000-4-5 Prüfschärfegrad 2 Stoßspannungen unsymmetrisch: EN 61000-4-5 Prüfschärfegrad 3 Leitungsgebundene HF-Störungen: EN 61000-4-6 Prüfschärfegrad 3
EMV-Störaussendung	EN 55022: Class A FCC 47 CFR Part 15: Class A Germanischer Lloyd: Klassifizierungs- und Bauvorschriften VI-7-3 Teil1 Ed.2003
Festigkeit	Vibration EC 60068-2-6 Test FC Prüfschärfegrade nach IEC 61131-2 E2 CDV und Germanischer Lloyd Richtlinien für die Durchführung von Baumusterprüfungen Teil 1 Schock EC 60068-2-27 Test Ea Prüfschärfegrad nach IEC 61131-2 E2 CDV
Zertifizierungen	cUL 508 / CSA 22.2 No.142 erfüllt cUL 1604 / CSA 22.2 No.213 angemeldet Germanischer Lloyd erfüllt

Notes on CE identification

Die Konformitätserklärungen werden in Übereinstimmung mit den EU-Direktiven für die zuständigen Behörden an folgender Stelle bereitgehalten:

Innominate Security Technologies AG
Albert-Einstein-Str. 14
D-12489 Berlin
Telephone ++49 (0)30 6392-3300

FCC Note

This equipment has been tested and found to comply with the limits for a Class A digital device, persuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.